



# State Official's Guide

## Critical Infrastructure Protection



The Council of State Governments



# **State Official's Guide to Critical Infrastructure Protection**

by Barry Hopkins



The Council of State Governments

Copyright 2003, The Council of State Governments  
Manufactured in the United States of America  
ISBN #0-87292-815-2 ■ Price: \$35.00

All rights reserved.

Inquiries for use of any material should be directed to:  
The Council of State Governments, P.O. Box 11910, Lexington, KY 40578-1910

CSG's Publications Sales Department: 1-800-800-1910



The Council of State Governments  
*Preparing states for tomorrow, today . . .*

The Council of State Governments (CSG), the multibranch organization of the states and U.S. territories, prepares states for tomorrow, today, by working with state leaders across the nation and through its regions to put the best ideas and solutions into practice. To this end, CSG:

- Interprets changing national and international conditions to prepare states for the future.
- Advocates multistate problem-solving and partnerships.
- Builds leadership skills to improve decision-making.
- Promotes the sovereignty of the states and their role in the American federal system.

**Council Officers**

*President:* Gov. Frank Murkowski, Alaska

*Chair:* Sen. John Hottinger, Minn.

*President-Elect:* Gov. Ruth Ann Minner, Del.

*Chair-Elect:* Assemblyman Lynn Hettrick, Nev.

*Vice President:* Gov. Jim Douglas, Vt.

*Vice Chair:* Sen. Earl Ray Tomblin, W. Va.

**Headquarters**

Daniel M. Sprague, Executive Director  
Albert C. Harberson, Director of Policy  
2760 Research Park Drive  
P.O. Box 11910  
Lexington, KY 40578-1910  
Phone: (859) 244-8000  
Fax: (859) 244-8001  
Internet: [www.csg.org](http://www.csg.org)

**Washington, D.C.**

Jim Brown, Director  
444 N. Capitol Street, NW, Suite 401  
Washington, DC 20001  
Phone: (202) 624-5460  
Fax: (202) 624-5452

**Eastern**

Alan V. Sokolow, Director  
40 Broad Street  
Suite 2050  
New York, NY 10005  
Phone: (212) 482-2320  
Fax: (212) 482-2344

**Midwestern**

Michael H. McCabe, Director  
614 E. Butterfield Road, Suite 401  
Lombard, IL 60148  
Phone: (630) 810-0210  
Fax: (630) 810-0145

**Southern**

Colleen Cousineau, Director  
1946 Clairmont Rd.  
Atlanta, Ga 30033  
Phone: (404) 633-1866  
Fax: (404) 633-4896

**Western**

Kent Briggs, Director  
1107 9th Street, Suite 650  
Sacramento, CA 95814  
Phone: (916) 553-4423  
Fax: (916) 446-5760

## Foreword

As a result of the September 11, 2001 terrorist attacks, states were awakened to the necessity of securing critical infrastructure and assets, important to the health, wealth and security of our nation, that were suddenly seen as vulnerable. Both the significance and complexity of this task is staggering given the enormous array of critical infrastructure, both publicly and privately owned, and assets, both physical and virtual, that spans the states.

Indeed, states are faced with many questions as they work to protect our nation's various critical infrastructures. What/where are the most important assets? What critical infrastructures within our state are dependent on those in neighboring states? How do we best coordinate protection efforts with neighboring states? How do we effectively secure critical assets yet not interfere with the flow of commerce? What are the legal issues regarding sharing information when protecting critical infrastructure?

We are pleased to introduce the State Official's Guide to Critical Infrastructure Protection as a tool that can aid state policy makers in their decisions regarding the protection of critical infrastructure and assets. The Guide is intended to be a resource to help policymakers understand the myriad of issues that arise when addressing infrastructure protection issues, the roles that states must play in protection efforts and the considerations that must be made when determining protection strategies.

The Guide introduces state officials to the variety of issues surrounding critical infrastructure protection and outlines factors that should be considered when making policy decisions regarding various infrastructure sectors. In addition, rather than prescribing specific policy, the Guide provides valuable information aimed at enabling state leaders to determine the strategies best suited to their state's circumstances and infrastructure portfolio. Finally, the Guide offers state officials various policies and practices as examples that may be put to use in their respective states.

CSG would like to thank the various state officials who gave their insights on the issues highlighted within this Guide. And, thanks also go to members of the Critical Infrastructure Advisory Board for their guidance and input.



Daniel M. Sprague  
Executive Director  
The Council of State Governments



## Table of Contents

Foreword .....	i
Acknowledgements .....	v
Executive summary .....	vii

### Chapter One

What do you need to know about critical infrastructure protection? .....	1
What is critical infrastructure and why is it critical? .....	3
The history of critical infrastructure protection .....	4
What are the critical infrastructure sectors for states? .....	7

### Chapter Two

What must you consider when making critical infrastructure policy? .....	19
What are the challenges to protecting the various infrastructures? .....	21
What are the roles of federal and state government and the private sector? ..	37
What are the legal aspects of critical infrastructure protection? .....	42

### Chapter Three

What are states currently doing and what future action is necessary? .....	45
What are states doing to protect critical infrastructure? .....	47
What can states do in the future? .....	54
Conclusion .....	55

### Appendices

Appendix A: Critical Infrastructure Acronyms .....	59
Appendix B: Glossary of terms .....	69

## List of Tables and Figures

### Figure 1

Ridership by Transit Mode, 2000 ..... 15

### Figure 2

Interdependence of Energy and Other Critical Infrastructures ..... 26

### Figure 3

Vulnerability of Oil Sector from Production to Delivery ..... 28

### Figure 4

Vulnerability of Natural Gas Sector from Production to Delivery ..... 29

### Figure 5

Transportation Sector Stakeholders ..... 31

### Figure 6

Number of Chemical Facilities with “Worst-Case Release” Potential ..... 37

### Figure 7

Federal Government Organization for Protection of Critical Infrastructure .. 40

## Acknowledgements

Funding for the *State Official's Guide* series is provided in part by The Council of State Governments' 21st Century Fund. The 21st Century fund is an internal foundation operating within the Council's 501(c)(3) organization. The purpose of the fund is to strengthen the Council's policy and research capacity by supporting innovative and entrepreneurial approaches to product development. Contributors include:

- American Express Company
- BP America
- DuPont
- Eastman Kodak Company
- GlaxoSmithKline
- Intuit
- Loeffler Jonas & Tuggey LLP
- Metabolife International, Inc.
- Pfizer, Inc.
- Pharmacia Corporation
- Philip Morris Management Corporation
- PhRMA
- The Procter & Gamble Company
- R.J. Reynolds Tobacco Company
- SBC Communications, Inc.
- 3M
- United Parcel Service
- USAA
- Wyeth

### **Private Sector Collaborative Principles**

The Council of State Governments (CSG) is the only national organization serving every elected and appointed official in all three branches of each state and territorial government. Since 1933, CSG has championed excellence in state government by advocating multi-state problem solving and states' rights by recognizing and tracking national trends, identifying innovations, and through nonpartisan groundbreaking leadership training and support. CSG performs this work through its national office, as well as regional offices based in the East, Midwest, South and West.

CSG's activities are supported by state dues as well as federal government, foundation and private-sector funding. Work performed and products produced by CSG are designed to benefit CSG members and to meet the most stringent standards of quality and integrity without regard to funding source.

## Executive Summary

### What is critical infrastructure and why is it critical?

The health, wealth and security of our nation are heavily tied to the continued production and distribution of certain commodities and services. Therefore, the array of infrastructures and assets around which this production and distribution occur are deemed vital to our country. These “critical infrastructures” – whether publicly or privately owned, whether physical or virtual – are necessary to sustain important social and economic activities. While never specifically defined until the last decade, examples of such critical infrastructure include transportation systems, energy and pipeline systems, banking and finance, public health/emergency services, water systems, government and agriculture.

The USA Patriot Act, anti-terror legislation passed six weeks after the September 11 attacks, established measures to allow, among other priorities, for the further protection of critical infrastructure sectors. The act defined critical infrastructure as “systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.” Developed by the president’s Office of Homeland Security, *the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released in February 2003, defined specific sectors as critical infrastructures under the guidelines of the USA Patriot Act.<sup>1</sup> The following sectors constitute the critical infrastructure sectors for states:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Telecommunications and Information Systems
- Energy
- Transportation
- Banking and Finance
- Chemical Industry<sup>2</sup>

After September 11, states and the federal government emphasized the development and implementation of plans that would protect this infrastructure from disruption due to man-made attacks or natural disasters. The list above shows that America’s critical infrastructure sectors provide the goods and services that contribute to a strong national defense and a thriving economy. More than that, their continued operation, reliability and resiliency create a sense of confidence and help shape our sense of identity and purpose. They also frame our way of life and enable Americans to function as a society and enjoy one of the highest standards of living in the world. Together these industries ensure the following:

- production, delivery and distribution of essential goods and services
- interconnectedness and communications

<sup>1</sup>The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003, 6.

<sup>2</sup>From the list defined in the national strategy document, we have excluded the defense, government, and postal and shipping sectors. While all are important to our economy and national security, they are deemed less relevant within the framework of a state policy discussion. The defense sector does not apply evenly to all states; the postal sector is federally controlled; all states presumably have plans regarding the continuity of government so its discussion here is irrelevant; and, the shipping sector is heavily tied to the transportation sector, which is later covered in detail.

- reliability of services
- public safety and security

Critical infrastructure sectors such as agriculture, food, water, public health and emergency services provide the essential goods and services that Americans depend on to survive. Energy, banking and financial services, chemical manufacturing, shipping and transportation help sustain our economy and make a wide variety of goods and services possible and available. Information and telecommunications infrastructures not only allow the communications necessary to conduct everyday life, they also connect and increasingly control the operations of other critical infrastructures. And emergency services, public health infrastructure and government institutions help guarantee our health, safety, national security, freedom and governance.

All of these infrastructures are basic components of our daily lives that we notice only when service is disrupted. Therefore, when disruption does occur, we expect reasonable explanations and speedy restoration of service.

### **What must you consider when making infrastructure protection policy?**

The technological sophistication of our society and institutions presents terrorists with many potential targets. Since the concept of critical infrastructure protection is relatively new, much of the expertise required to plan for and ensure the protection of critical infrastructures lies outside the federal government, including much of the knowledge about what specifically needs to be protected. In effect, responsibility for the defense of critical infrastructures is shifted down to state and local governments and private sector stakeholders that make up the various infrastructure sectors. Therefore, it is necessary for state leaders to realize the challenges associated with securing each of the individual sectors.

Critical infrastructure protection is a complex mission that involves a broad range of functions performed throughout government and the private sector. Because infrastructure protection encompasses such a broad scope, it is foolish to think everything can be fully protected; therefore national preparedness and response must also be part of our strategy. This combined focus – critical infrastructure protection and incident response – encompasses activities related to national defense, law enforcement, transportation, emergency management, food safety, public health, information technology and other areas. Therefore, for critical infrastructure protection efforts to come even close to being successful, federal, state and local governments and private industry have specific roles and functions that must be integrated.

While the federal government is responsible for broad national security issues, responsibilities regarding emergency management, local coordination and regulatory issues have historically fallen upon state and local governments. However, given the resources that are necessary to protect the various infrastructure sectors, the range of governmental services that could be affected, and the necessity of private sector involvement in preparing for and mitigating risks, state and local resources alone are insufficient to meet all threats. In addition, private industry owns and operates approximately 85 percent of our critical infrastructures. Therefore, each critical infrastructure owner/operator's unique capabilities, expertise and resources are necessary for a comprehensive national protection effort.

A range of legal and administrative activity has emerged regarding critical infrastructure protection since September 11 under the auspices of homeland security. The legal framework of critical infrastructure protection is a moving target that continues to change. Indeed, the scope of these legal issues and the range of perspectives on critical infrastructure protection are vast. Much of this is spurred by the fact that the U.S. landscape of critical infrastructure today is characterized by an intertwining of government and industry. Each sector has its own responsibilities, interests and concerns.

The law as it applies to critical infrastructure protection involves statutes enacted by Congress and state legislatures, and regulations promulgated by federal and state government agencies, many of which were put in place to address specific issues that are characteristic of each regulated area. Therefore, many parties have jurisdiction to make law concerning some part of the nation's critical infrastructure. The legal issues that states are currently dealing with when making critical infrastructure policy stem almost completely from issues regarding information sharing, including questions regarding information protection, privacy, right-to-know issues, anti-trust issues, and even liability issues.

### **What are the states currently doing and what future action is necessary?**

To begin to address the many policy issues that arise when considering critical infrastructure protection, it will be helpful for state officials to know what states are currently doing in this area. Unfortunately, states' responses to critical infrastructure issues have been somewhat limited due to the following issues:

- infrastructure protection as a new concept
- information sharing problems
- more focus on response than on protection
- budget problems.

States are attempting to do more, but due to these limiting factors they have only been able to successfully address critical infrastructure protection through two ways: legislation and partnerships.

States are doing many things to address critical infrastructure protection, but there is room for additional action. States should take steps to do the following:

- Focus on coordination, communication and information sharing efforts
- Focus on partnerships with other states, the federal government and the private sector
- Conduct scenario-based exercises
- Work on risk assessments and identifying critical assets and vulnerabilities

As states work to address the many infrastructure protection challenges, it is important to remember the complex nature of the infrastructures and assets that are to be protected. As potential targets for terrorists, the United States' critical infrastructures are a highly diverse, interdependent mix of facilities and networks. Governments own and operate some of them, but most are controlled by the private sector. However, all are vulnerable in some way to the terrorist threat. And they are a network of interdependent systems. Failure in one infrastructure can cascade to cause disruption or failure in others, and the consequences for states and the public can be massive. States must understand the challenging complexities as they work to implement future strategies and plans to protect critical infrastructure.



## Chapter One



What do you need to know about Critical Infrastructure Protection?

## What is critical infrastructure and why is it critical?

The nation's economic vitality, national security and quality of life of its citizens depend to a certain degree upon the availability, continuous operation and reliability of several different infrastructure sectors, both physical and "virtual." Since these various sectors provide the framework around which we live our daily lives, conduct business and function as a society, they are deemed critical to our country's existence.

In recent months, public and private officials in the United States have spoken and written more frequently about critical infrastructure protection. Yet not too long ago, most citizens and government officials were unfamiliar with the concept. So why is so much attention now being given to this issue?

The attacks of September 11 heightened awareness of our nation's vulnerabilities and the necessity to secure our critical infrastructure, not just from future terrorist attacks, but from all major disasters and events that could disrupt and threaten our way of life. To this end, President Bush's Office of Homeland Security (now the Department of Homeland Security) developed the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which defines the following sectors as critical infrastructures under the guidelines of the USA Patriot Act:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Defense Industrial Base
- Government
- Telecommunications and Information Systems
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping<sup>3</sup>

These sectors provide the goods and services that contribute to a strong national defense and a thriving economy. More than that, their continued operation, reliability and resilience create a sense of confidence and help shape our sense of identity and purpose. They also frame our way of life and enable Americans to function as a society and enjoy one of the highest standards of living in the world. Together these industries ensure the following:

- production, delivery and distribution of essential goods and services
- interconnectedness and communications
- reliability of services
- public safety and security

Critical infrastructure sectors such as agriculture, food, water, public health and emergency services provide the essential goods and services that Americans depend on to survive. Energy, banking and financial services, chemical manufacturing, shipping and transportation help sustain our economy and make a wide variety of goods and services possible and available. Information and telecommunications infrastructures allow the communications neces-

---

**Critical infrastructures provide the goods and services that contribute to a strong national defense and a thriving economy.**

---

<sup>3</sup>The White House, *National Strategy for the Physical Protection of Critical Infrastructure*, 6.

---

**Critical infrastructure protection pertains to the proactive activities aimed at protecting those physical and virtual systems that are defined by the USA Patriot Act and the national strategy for physical protection as those “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”**

---

sary to conduct everyday life as well as connect and increasingly control the operations of other critical infrastructures. And, emergency services, public health infrastructure and government institutions help guarantee our health, safety, national security, freedom and governance.

Critical infrastructure protection pertains to the proactive activities aimed at protecting those physical and virtual systems that are defined by the USA Patriot Act and the national strategy for physical protection as those “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” These activities deter or prevent attacks against critical infrastructures by people (such as terrorists, other criminals or hackers), by nature (such as hurricanes, tornadoes, earthquakes or floods), and by accidents involving nuclear, biological or chemical substances.

Protecting these infrastructures is extremely important because when we interact with them we expect results – when flipping a switch, we expect light; when using a faucet, we expect water; when using a phone, we expect to be able to make a call. All of these infrastructures are basic components of our daily lives that we notice only when service is disrupted. The 2003 Blackout, which left as many as 50 million people in the Northeast, parts of the Midwest and Ontario without electricity, brought these issues to the fore. Its aftermath has brought many questions as to why it happened and demands for solutions to make sure it does not happen again. When disruption does occur, we expect reasonable explanations and speedy restoration of service.

## **The history of critical infrastructure protection**

Until recently, the concept of critical infrastructure had no agreed upon standard or definition in terms of policy. Until the issues of terrorism and homeland security were thrust upon us with the attacks of September 11, critical infrastructure referred mainly to our virtual systems and information infrastructure. Many people may not consider the basic concept of critical infrastructure as a new one for the United States, as we have greatly relied on various systems throughout at least the last century to sustain our way of life – including the Interstate highway system beginning in the 1960s, the rail systems since the Industrial Revolution, and the postal system for over a couple hundred years. Even as late as the 1980s, the debate surrounding infrastructure focused not on protection so much as its condition, as many people believed that our roads, bridges, water systems and dams were in a state of crisis. However, the history of modern critical infrastructure protection as we know it today can really be traced back through the last decade, with the events of September 11 providing a sharper focus.

### **Critical Infrastructure Protection before September 11**

During the 1990s, as our physical infrastructure became increasingly connected and controlled by a “virtual infrastructure,” the Internet, computers and telecommunications helped give birth to the concept of critical infrastructure. From this grew questions of vulnerability related to such reliance on computer networks to maintain and operate many areas of our critical infrastructure. This mainly began in the early 1990s, when a study by the Defense Science Board stressed the need to create a presidential commission to explore threats and vulnerabilities of critical infrastructures. Shortly thereafter, in July 1996, President Clinton established the President’s Commission on Critical Infrastructure Protection (PCCIP).<sup>4</sup>

In 1997, the PCCIP released its report to President Clinton.<sup>5</sup> The commission found no immediate threats to the nation’s infrastructures, but it recognized that there were vulnerabili-

<sup>4</sup>William J. Clinton, “Critical Infrastructure Protection,” Executive Order 13010, 17 July 1996, *Federal Register*, vol. 61, no. 138, 3747-3750.

<sup>5</sup>President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructures*, October 1997.

ties due to the ever-increasing rates of interconnection occurring across information and telecommunication systems. In May 1998, President Clinton released Presidential Decision Directive No. 63, which established groups within the federal government to develop and implement plans that would protect government-operated infrastructures and develop a National Infrastructure Assurance Plan to protect the nation's entire network of critical infrastructure by the year 2003.<sup>6</sup> This directive called for both physical and cyber protection, but focused more on cyber protection from "hacker-attacks." Although the structure of the government's critical infrastructure protection efforts is different today, the directive created the following entities:

- **Critical Infrastructure Coordination Group** – The primary interagency group for developing and implementing policy and coordinating the federal government's own security measures.
- **National Infrastructure Assurance Council (NIAC)** – A panel of private operators of infrastructure assets and officials from state and local governments and federal agencies.
- **Critical Infrastructure Assurance Office (CIAO)** – Supported individual agencies in developing plans, helped coordinate national education and awareness campaigns and provided legislative and public affairs support.
- **National Infrastructure Protection Center (NIPC)** – An expansion of the FBI's computer crime division into a focal point for national threat assessments, vulnerability analysis, investigations and response coordination in the information systems and computing sectors.
- **Information Sharing and Analysis Centers** – ISACs, run by the private sector, act as the information-sharing conduits between the different levels of government and the private sector.

The president's directive established a structure for implementing critical infrastructure policy that carried through the establishment of the Department of Homeland Security, with some elements continuing today. The directive was the first initiative that required the federal government to begin developing plans regarding analyzing and correcting infrastructure vulnerabilities, warning, response, reconstitution, research and development, intelligence collection, education, and legislative and budgetary requirements.

However, from 1998 until the September 11 attacks, federal critical infrastructure protection efforts focused too heavily on securing information systems and the Internet, as PDD-63 emphasized. Therefore, while the directive established critical infrastructure protection as a national priority and created a structure for its implementation, it was not pursued in a manner sufficient to meet the growing threat of terrorism.

### Critical Infrastructure Protection Post-September 11

After September 11, states and the federal government placed more emphasis on developing and implementing plans that would protect critical infrastructure from disruption due to man-made attacks or natural disasters. Five weeks after the September 11 attacks, the Bush administration released Executive Order 13231 (EO 13231), which established the administration's initial policy on critical infrastructure protection. It called for the nation "to protect against the disruption of the operation of information systems for critical infrastructure and thereby help protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."<sup>7</sup> EO 13231 also created the following entities:

<sup>6</sup>The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998.

<sup>7</sup>George W. Bush, "Critical Infrastructure Protection in the Information Age," Executive Order 13231, 16 October 2001, < <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html> > (11 June 2003).

---

**After September 11, states and the federal government placed more emphasis on developing and implementing plans that would protect critical infrastructure from disruption due to man-made attacks or natural disasters.**

---

- **President's Critical Infrastructure Protection Board** – Comprised of members of the senior executive staff and chaired by the special advisor to the president for cyberspace security, the board is responsible for recommending policies and programs for protecting information systems for critical infrastructures.
- **National Infrastructure Advisory Council** – Comprised of members of the private sector, the council is responsible for providing the president with advice on the security of information systems.<sup>8</sup>

Not long after September 11, President Bush also signed Executive Order 13228 (EO 13228), which established the Office of Homeland Security. Among other duties, the office was to “coordinate efforts to protect the U.S. and its critical infrastructures from the consequences of terrorist attacks.” The order directed the office to “coordinate efforts to protect critical infrastructures ... and ... work with federal state, and local agencies and private entities to:

- strengthen measures for protecting energy production, transmission and distribution services and critical facilities; other utilities; telecommunications;
- coordinate efforts to protect critical public and privately owned information systems;
- protect transportation systems within the United States; and
- protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption.”<sup>9</sup>

Shortly thereafter, Section 106 of The USA Patriot Act (P.L. 107-56), called the Critical Infrastructures Protection Act of 2001, established measures to help protect critical infrastructure sectors. The act defined critical infrastructure as “systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.”<sup>10</sup> This act came to define the infrastructure areas that are deemed critical.

The following year, the Homeland Security Act of 2002 (P.L. 107-296) established the Department of Homeland Security. Critical infrastructure protection efforts were consolidated within the new department and all of the relevant federal agencies and organizations were transferred into the department's Information Analysis and Infrastructure Protection Directorate (IAIP), including the following:

- The National Infrastructure Protection Center (NIPC)
- The Critical Infrastructure Assurance Office (CIAO)
- The National Infrastructure Simulation and Analysis Center (NISAC)
- FedCIRC, the federal civilian government's unit for computer security incident reporting and assistance with incident prevention and response
- The Department of Energy's Energy Security and Assurance Program
- The National Communications System (NCS)

The consolidation was intended to bring responsibility for policy, planning, analysis and warning under one department, thereby facilitating coordination with state and local governments and the private sector, and to combine the agencies that were formerly responsible for most of the “broad-brush” aspects of federal critical infrastructure protection policy.

<sup>8</sup>Now managed by the Department of Homeland Security.

<sup>9</sup>George W. Bush, “Establishing the Office of Homeland Security and the Homeland Security Council,” Executive Order 13228, 8 October 2001, Federal Register, vol. 66, no. 196, 51812-51817.

<sup>10</sup>H.R. 3162-130 (P.L. 107-56), Section 1016(e), < <http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf>> (30 June 2003).

Under the IAIP Directorate, these agencies were merged into six offices:

- The Infrastructure Coordination Division
- The Infrastructure Protection Division
- Competitive Analysis and Evaluation Office
- Planning and Partnerships Office
- The Risk Assessment Division
- The Information and Warnings Division

In addition to creating the Department of Homeland Security and consolidating agencies into the IAIP Directorate, the Bush administration issued a series of national strategies that addressed critical infrastructure protection:

- The National Strategy for Homeland Security (July 2002)
- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)
- The National Strategy to Secure Cyberspace (February 2003)

## What are the critical infrastructure sectors for states?

The following section will briefly highlight the critical infrastructure sectors and examine the characteristics and classification of each, except for the defense industrial, government, and postal and shipping sectors. The defense sector, while important to our economy and national security, is not relevant to the state policy discussion that will follow in subsequent sections, and neither is the postal sector, which is a federal entity with federally controlled facilities. All states presumably have plans regarding the continuity of government so it will not be dealt with here. And, the shipping sector will be covered under the transportation sector.

### Agriculture/Food

Our nation's agriculture and food systems and the industries that comprise this sector are a source of important commodities in the United States, and they account for close to one-fifth of the gross domestic product.<sup>11</sup> In addition, this sector contributes heavily to our export economy, as the United States exports approximately one quarter of its farm and ranch products. The industry systems that make up this sector include the following:<sup>12</sup>

- supply chains for feed, animals and animal products
- crop production and its associated supply chains (seed, fertilizer and related materials)
- post-harvesting components of the food supply chain, including processing, production, packaging, and storage and distribution
- retail food sales, institutional food services, and consumption (restaurant and home)

Increasingly, more of our food is grown abroad, foodstuffs are transported long distances, and dining out has become a way of life. These aspects of the way that food is produced, distributed and consumed present challenges for ensuring its safety and security. Maintaining public confidence in the safety of agricultural and food systems is key not only to the economic viability of these industries but also to maintaining a sense of sociological order. In addition, the United States' reputation as a reliable supplier of safe, high quality agricultural and food products is likewise essential to maintaining the confidence of foreign customers who are important to states' economies and the national economy as a whole.

<sup>11</sup>U.S. Bureau of Economic Industry Analysis, "Industry Accounts Data," <http://www.bea.doc.gov/bea/dn2/gpoc.htm>, (13 February 2003).

<sup>12</sup>Drawn from the National Strategy for the Physical Protection of Critical Infrastructure document.

### Critical Infrastructure for States

- Agriculture and Food
- Water
- Public Health and Emergency Services
- Telecommunications and Information Systems
- Energy
- Transportation
- Banking and Finance
- Chemical Industry

## Water

Water infrastructure systems consist of two broad components: fresh water supply and wastewater treatment. These systems include the following:

- surface and ground sources of water that supply municipal, industrial, agricultural and consumer needs
- dams, reservoirs, aqueducts, and pipes that store and transport water
- water distribution systems for users
- raw water treatment facilities that remove contaminants
- wastewater collection and treatment facilities

Across the country, these systems are comprised of a vast network of water infrastructure facilities that include the following:

- more than 75,000 state and locally owned dams and reservoirs;
- 1,800 federal reservoirs;
- more than 700,000 miles of drinking water networks (more than four times longer than the National Highway System);
- approximately 54,000 community drinking water systems consisting of more than 170,000 public drinking water facilities supplying water to more than 250 million Americans; and
- more than 16,000 publicly owned wastewater treatment facilities.<sup>13</sup>

These facilities are both publicly and privately owned and managed. The federal government owns hundreds of dams and other water diversion structures, but the vast majority of the nation's water infrastructure is either privately owned or owned by state or local governments. These public water systems are the most important to the nation because they provide fresh water, yet they are the most distributed and most dependent on other facets of the water sector. They depend on reservoirs, dams, wells and aquifers, as well as treatment facilities, pumping stations, aqueducts and transmission pipelines.

Water sector infrastructures are diverse, complex and distributed, ranging from systems that serve only a few customers to those that serve millions. Water supply and water quality are extremely critical to public health and the national economy. Damage or destruction within this sector could affect public health by disrupting the delivery of vital human services, contaminate the environment, and lead to loss of life through poisoning and contamination.

## Public Health and Emergency Services

These large and diverse sectors share a basic function: saving lives and protecting the public. The public health sector consists of a variety of entities and institutions, including more than 5,800 registered hospitals.<sup>14</sup> Made up of state and local health departments, health clinics, mental health facilities, hospitals, nursing homes, mortuaries, supply facilities, laboratories and pharmaceutical stockpiles, the public health system plays a critical role in ensuring the health and well-being and, in times of disaster, the recovery of the population. Likewise, the emergency services sector is vital to the public health and safety. Emergency services consist of fire, rescue, emergency medical service (EMS), and law enforcement organizations from more than 87,000 U.S. localities. These professionals save lives and property in the

<sup>13</sup>Congressional Research Service, Terrorism and Security Issues Facing the Water Infrastructure Sector; Document #RS21026 (Washington, D.C.: Library of Congress, May 2003), 2; American Public Works Association, "Facts About America's Critical Infrastructure Derived from Federal Sources," <<http://www.apwa.net/GovtAffairs/Infrastructure/>> (22 July 2003).

<sup>14</sup>The White House, National Strategy for the Physical Protection of Critical Infrastructure, 9.

event of an accident, natural disaster, or terrorist incident.

Public health infrastructure is not only vital to all aspects of public health, it is also critical in the event of terrorist attacks. This infrastructure is not visible to the extent that highways and energy transmission lines are, but it is no less important. Hospitals, clinics and public health systems play a critical role in mitigating and recovering from the effects of disasters or deliberate attacks. Any physical damage or disruption experienced by these facilities – whether through a direct terrorist strike or as a result of secondary damage or nuclear, chemical or biological contamination – could not only be detrimental to the sector's response, but could also exacerbate an existing emergency. The same holds true for emergency services. Fire, rescue, EMS and law enforcement organizations play a key role during times of disaster or attack. Disruptions in any segment of this sector's ability to carry out its mission would cause additional damage or loss of life.

### **Telecommunications/Information Systems**

Telecommunications and information systems – the sectors that gave birth to the current concept of “critical infrastructure” – are no less a part of daily life than mundane tasks such as shopping, commuting to work, bathing and eating. In fact, one is hard-pressed to find a facet of daily life that is not in some way affected or facilitated by these sectors. Physical telecommunications systems and cyberspace make up the backbone of much of our country's economy and society.

Telecommunications systems and cyberspace provide the network over which much of the economic activity and essential services flow and are controlled. Basic voice and data services are provided to public and private users through the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks, encompassed by a complex and diverse networked infrastructure. The PSTN consists of more than 20,000 switches, circuits, access provider switching systems, and a morass of other equipment that provides circuits for telephone, data and point-to-point services. Made up of a few billion miles of fiber optic and copper cable, the network is the backbone of telecommunications infrastructure, with cellular, microwave and satellite technologies providing extended gateways to the network for mobile users. Supporting this underlying physical network are systems that provide the necessary management and administrative functions, such as billing, accounting, configuration and security management.<sup>15</sup>

The Internet provides the virtual pathway, or cyberspace, that is made possible by this physical infrastructure and hundreds of thousands of interconnected routers, switches, cables and computers. Advances in data network technology and the increasing demand for services to move data gave birth to the Internet infrastructure. The Internet consists of a global network of networks that use a common set of protocols. Internet Service Providers (ISPs) provide end-users with access to the Internet. Larger ISPs link them through network access points. Smaller ISPs provide regional and local Internet access to end-users via the PSTN, using transmission capacity leased from the larger ISPs.

Cyberspace is the nervous system of many other infrastructure sectors. Agriculture, water, public health, emergency services, government, energy, transportation, banking and finance, and others all depend on it to conduct operations. Therefore, cyberspace is the control system of our country. Today there are 109.5 million Internet hosts on the World Wide Web compared to 6.6 million hosts five years ago. More than 62 percent of all U.S. households are now online and 73.1 percent of all Internet users visit e-commerce sites. In 2000, more than 49 million personal computers were shipped, and this will continue to increase.<sup>16</sup> The

<sup>15</sup>The White House, National Strategy for the Physical Protection of Critical Infrastructure, 47.

<sup>16</sup>Don Heiman, National Association of State Chief Information Officers, Public-Sector Information Security: A Call to Action for Public-Sector CIOs (Lexington, KY: National Association of State Chief Information Officers, October 2002), 6.

---

**Energy policy and energy security are important to policy-makers because of energy's impact on public health, the environment, the economy and our security.**

---

world is obviously becoming more tightly interconnected via the Internet and telecommunications systems.

Our economy and national security depend upon cyberspace and telecommunications systems to function and ensure essential services and networks. Much of the physical network has been put in place and is owned by the private sector. However, the importance of these networks to our socioeconomic order and security cannot be discounted. Without them, many essential services and operations, including our economy, would suffer severely.

## **Energy**

Energy drives many of the processes behind American society and it is essential to our economy, national security, and quality of life. Technological innovation, information systems, industrial achievements, and the construction of vast capital markets and financial systems all require energy. Without it, much of our society and economy today would be impossible. Energy policy and energy security are important to policy-makers because of energy's impact on public health, the environment, the economy and our security.

The energy sector is commonly divided into two segments in the context of critical infrastructure protection: electricity and oil and natural gas. However, due to its importance to states in terms of energy production, for the purposes of this guide, we will add a third sector: nuclear plants.<sup>17</sup>

## **Electricity**

The U.S. electric system is comprised of an interconnected network of generating plants, transmission lines and distribution facilities. The industry services almost 130 million households and institutions, and the system's transmission grid consists of nearly 160,000 miles of high voltage transmission lines.

The North American electric system is an interconnected, multinodal distribution system that supplies power not only to the United States, but also to Canada and a portion of northern Mexico. This physical system is comprised of three major parts:

- generation facilities
- transmission and distribution systems
- control and communications systems

Generation assets include fossil fuel plants, hydroelectric dams and plants, and nuclear power plants. Transmission and distribution systems link these generation systems to the national power grid. Transmission and distribution systems are in turn managed by control and communication systems that control the flow of electricity into industrial plants, commercial businesses and homes. In addition, the electric infrastructure is also comprised of secondary facilities and systems that deliver fuel supplies necessary to generate electricity. Telecommunications and transportation components are also a big part of the electricity sector.

The United States generated approximately 3.8 trillion kilowatt hours of electricity in 2002.<sup>18</sup> This is a staggering amount of power, used to support many facets of our society, including homes, schools, hospitals, businesses and manufacturing plants. Therefore, if the United States experienced a widespread or long-term disruption of the power grid, many of the activities critical to our economy and security would be next to impossible.

<sup>17</sup>The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets lists nuclear plants under the classification "key asset." However, as stated above, due to the fact that nuclear plants are more relevant and important to states in terms of energy than as a "key asset," they will be covered in the energy section.

<sup>18</sup>Edison Electric Institute, "Statistical Highlights," [http://www.eei.org/industry\\_issues/industry\\_overview\\_and\\_statistics/statistical\\_highlights/](http://www.eei.org/industry_issues/industry_overview_and_statistics/statistical_highlights/) (29 July 2003).

## Nuclear Plants

Commercial nuclear power plants provide 20 percent of the country's electricity supply, producing more electricity than is required to meet the total electric demand in all but three countries in the world.<sup>19</sup>

The United States has 104 commercial nuclear reactors in 31 states. The Nuclear Regulatory Commission (NRC) regulates these reactors and other civilian nuclear facilities, materials and activities. With the aid of federal regulations, the NRC has required for over 25 years that these facilities maintain rigorous security programs to withstand attacks. In addition, the plant operator must have an on-site emergency response plan approved by the Federal Emergency Management Agency, an on-site plan to address the safety of plant workers in an emergency, and established procedures for shutting down the plant. The NRC also requires the following security measures for nuclear power plants:

- intrusion detection devices
- access barriers
- fenced perimeters
- armored defensive positions
- armed and trained guard forces
- detailed personnel background checks
- a comprehensive defense strategy<sup>20</sup>

In terms of energy infrastructure, nuclear power plants are among the most hardened to threats. In fact, due to NRC requirements, they are extremely hardened physically, designed to withstand hurricanes, tornadoes, earthquakes and other disasters. The potential damage that could result from an attack or catastrophic event at a nuclear facility highlights the importance of these measures.

## Oil and Natural Gas

The petroleum sector consists of a diverse and lengthy supply chain. Our country's oil infrastructure includes five main components:

production (including exploration, field development, on- and offshore production, field collection systems and production support infrastructure)

- crude oil transport
- refining
- product transport and distribution
- control and support systems

The natural gas sector is as diverse and widely distributed as the oil industry. It consists of the following major components:

- production (including exploration, field development, on- and offshore production, field collection systems and production support infrastructure)
- transmission
- local distribution

The oil and natural gas industries are closely integrated, since both substances are often

<sup>19</sup>United States Energy Association, National Energy Security Post 9/11 (Washington, D.C.: United States Energy Association, June 2002), 41.

<sup>20</sup>National Conference of State Legislatures, Energy Security, (Denver: National Conference of State Legislatures, April 2003), 15.

---

**Commercial nuclear power plants provide 20 percent of the country's electricity supply, producing more electricity than is required to meet the total electric demand in all but three countries in the world.**

---

**The U.S. transportation system includes approximately 3.9 million miles of roads, more than 100,000 miles of rail, nearly 600,000 bridges, more than 300 ports, approximately 2.2 million miles of pipelines, 500 train stations and more than 5,000 public airports.**

discovered and produced together and are transported similarly by pipelines. The United States' oil and natural gas infrastructures and assets include the following:

- 880,000 oil wells
- 161 oil refineries
- 220,000 miles of oil pipeline
- 300,000 producing gas wells
- more than 1.3 million miles of natural gas pipeline and distribution lines
- 4,000 offshore platforms
- more than 600 natural gas processing plants
- 1,400 product terminals and 7,500 bulk stations<sup>21</sup>

The oil supply chain starts at the wellhead, continues through gathering lines, and is transported to refineries by ship or pipeline. Following the refining process, petroleum products are transported to large storage facilities, storage terminals and ports by pipelines, ships, barges or trucks. Ultimately, end products produced from petroleum, including gasoline and jet fuel, are distributed by truck to local gasoline stations and airports. More than 800 million gallons are moved each day.

The U.S. natural gas industry produces approximately 20 percent of the world's natural gas supply, delivering natural gas from the wellhead to the consumer through the three main components listed earlier. Production companies explore, drill and extract natural gas from the ground. Transmission companies operate the pipelines that link gas fields to major consumer areas. And local utilities, acting as distribution companies, deliver natural gas to individual customers. The number of natural gas consumers has grown through the years, and now totals more than 175 million Americans. Natural gas flows from more than 300,000 producing wells and is transported by about 180 natural gas pipeline companies to more than 1,200 gas distribution companies that serve all 50 states.

## Transportation

The United States maintains the world's largest and most complex national transportation system. It is comprised of a vast, interconnected network of modes, including the following:

- aviation
- highways and trucking
- maritime
- mass transit (buses, subways, ferry boats and light rail)
- pipeline
- rail (passenger and freight)

The U.S. transportation system includes approximately 3.9 million miles of roads, more than 100,000 miles of rail, nearly 600,000 bridges, more than 300 ports, approximately 2.2 million miles of pipelines, 500 train stations and more than 5,000 public airports.<sup>22</sup>

These transportation modes work together through an extensive network of infrastructure, operators, vehicles and vessels that permit movement throughout the system. Every day, the nation's transportation system moves more than 30 million tons of freight and provides

<sup>21</sup>Emily Frye, "Protecting Oil and Gas Infrastructures: A Classic Competitive Conflict Comes Face-to-Face with the Era of Terrorism," The CIP Report, vol. 1, (March 2003): 3.; The White House, National Strategy for the Physical Protection of Critical Infrastructure, 9.

<sup>22</sup>Governmental Accounting Office, Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO-03-843, 30 June, 2003, 2.

approximately 1.1 billion passenger trips.<sup>23</sup>

The size and function of the transportation sector make it vital to our economy and national security. Developed over decades of private and public investment, the various transportation modes provide the backbone over which goods and services move into, out of, and throughout the country. Just as important, transportation infrastructure provides convenient access and reliability to Americans as we move freely throughout the country.

### Aviation

Aviation in the United States is an intricate network with thousands of entry/exit points. The system includes hundreds of airports, thousands of planes and tens of thousands of daily flights. It has two main components:

- airports and the associated operating assets (including aircrafts and maintenance and fueling facilities)
- command, control, communications and information systems needed to operate and maintain U.S. airspace

### Highways and Trucking

Highways and trucking are fundamental components of the U.S. surface transportation infrastructure. Without this sector's resources, the movement of people, goods and services around the country would be much more difficult, expensive and time consuming. This sector includes the following:

- interstates and major U.S. highways
- roads (state highways, routes, secondary roads and rural roads)
- bridges
- tunnels
- trucks and buses
- intermodal terminals
- maintenance facilities, weigh-stations, rest stops and service areas
- roadway border crossings

### Maritime

The maritime shipping infrastructure provides another facet of our transportation system that facilitates the movement of goods into and out of the United States. This maritime infrastructure includes the following:

- ports and the associated operating assets
- coastal and inland waterways
- ships and passenger transportation systems
- locks, dams and canals
- network of railroads and pipelines that connect the maritime systems

The components of the maritime sector and its seaports vary widely in size, operation, ownership and purpose. The 361 U.S. ports are as diverse as the entities that use them. Many ships are privately owned and operated. State and local governments control some port facilities, while private corporations own and operate others. In addition, the federal government has

---

**The maritime sector is another main component of our economy and a hub of national and international activity. In fact, the U.S. maritime border is approximately 15 times longer than its land borders, with 95,000 miles of shoreline and a 3.4-million square mile exclusive economic zone.**

---

<sup>23</sup>ibid, 5.

---

**The military also depends heavily on railroads and the Department of Defense has designated more than 30,000 miles of rail as essential to national defense.**

---

designated some commercial seaports as strategic seaports because they can provide facilities and services necessary for military deployments.

The maritime sector is another main component of our economy and a hub of national and international activity. In fact, the U.S. maritime border is approximately 15 times longer than its land borders, with 95,000 miles of shoreline and a 3.4-million square mile exclusive economic zone.

### **Mass Transit**

The American mass transit system provides the public with a wide array of transportation services every day. Made up of a network of multiple-occupancy vehicle services designed to transport riders on a variety of local and regional routes, mass transit includes the following modes:

- buses
- heavy rail<sup>24</sup>
- commuter rail
- trolleys
- ferry boats
- light rail services

Each year, mass transit systems provide more than 9.5 billion passenger trips. In fact, mass transit carries more passengers each day than air or rail transportation, with buses as the most common form of transit. (See **Figure 1**). On the average workday, approximately 14 million Americans use some form of public transit.<sup>25</sup>

Mass transit systems vary in size and design, and each city and region has a unique system. Most are owned and operated by state and local agencies. About 6,000 agencies in the United States provide some form of transit services, such as buses, subways, light rail and ferries.<sup>26</sup> Most transit decisions and responsibility for transit safety and security are shared by private companies and a variety of government agencies at the federal, state and local levels.

### **Pipelines**

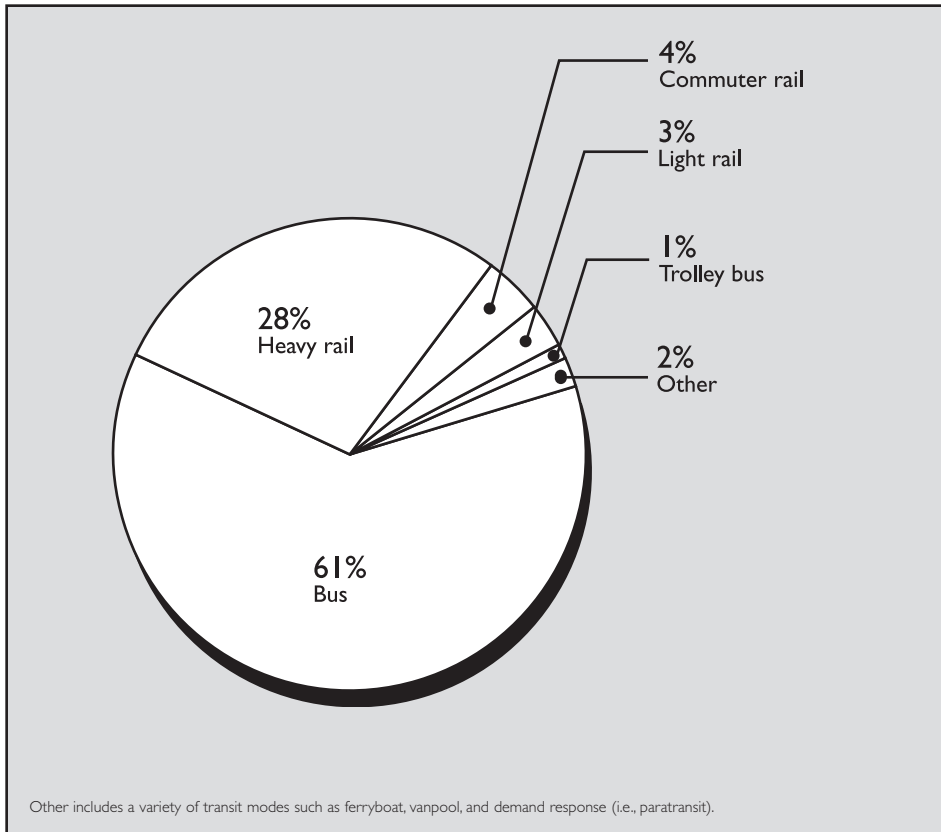
The pipeline sector, while extremely important to the energy sector, is considered more a part of the transportation infrastructure because of its function. Consisting of hundreds of thousands of miles of pipelines, above and below ground, the pipeline sector transports a variety of substances into, out of, and across the United States, including crude oil, refined petroleum products, natural gas and water.

### **Rail**

The rail sector provides an important service to the U.S. economy, linking producers, manufacturers and retailers. The railroad industry has operated in the United States for more than 175 years. Today, the rail sector carries approximately 40 percent of the ton-miles of freight over 123,000 miles of track, transporting mining, manufacturing and agriculture products; consumer goods; and liquid chemicals and fuels. In fact, trains carry more freight

<sup>24</sup>Heavy rail is defined here as a mode with the capacity for high volumes of traffic, characterized by high speed rail cars operating on fixed rails with separate right-of-way from other vehicular traffic. Most subway systems are considered heavy rail for statistical purposes.

<sup>25</sup>Governmental Accounting Office, Mass Transit: Challenges in Securing Transit Systems, GAO-02-1075T, 18 September, 2002, 1.

**Figure 1. Ridership by Transit Mode, 2000**

Source: American Public Transportation Association.

than any other mode of transportation.<sup>27</sup>

In addition, the military also depends heavily on railroads and the Department of Defense has designated more than 30,000 miles of rail as essential to national defense.<sup>28</sup> Therefore, the rail industry is critical not only to commerce, but also to national security.

### Banking and Financial Services

The U.S. financial services sector is considered a critical infrastructure by virtue of its importance to our economy and individual lives. This sector includes commercial banks, securities brokers and dealers, insurance companies, mutual funds, government-sponsored enterprises, pension funds, thrift institutions and others. It held more than \$23.5 trillion in assets as of the second quarter of 2002.<sup>29</sup> Some of the largest categories of financial institutions and their holdings are listed below:

- commercial banks (\$5.3 trillion)
- mutual funds (\$2.7 trillion)
- insurance companies (\$2.7 trillion)

<sup>27</sup>The CIP Report, vol. I (January 2003): I.

<sup>28</sup>ibid.

<sup>29</sup>Board of Governors of the Federal Reserve System, Federal Reserve statistical release, Flow of Funds Accounts of the United States: Flows and Outstandings Second Quarter 2002 (Washington, D.C.: Board of Governors of the Federal Reserve System, 16 September, 2002).

---

**The chemical sector is a critical national asset and a \$450 billion business that makes the following contributions to our economy: directly employs more than 1 million Americans, accounts for more than 5 million additional jobs in related industries such as agriculture, pharmaceutical, automotive and other industries, contributes \$97 billion in products to the health care sector alone and is the top U.S. exporting sector, accounting for 10 cents of every dollar in exports.**

---

- government-sponsored enterprises (\$2.2 trillion)
- pension funds (\$1.5 trillion)<sup>30</sup>

The banking and financial services infrastructure consists of physical structures, electronic infrastructure and, because of the highly specialized skills required by many financial services, human capital. While most activities and operations take place in large physical structures that require protection – including wholesale and retail banking operations, financial markets, regulatory institutions, and repositories for documents and financial assets – today’s financial utilities, such as payment and clearing and settlement systems, are primarily electronic. Although physical transfer of assets still takes place, this electronic infrastructure is an extremely large and growing component of this sector and includes computers, storage devices and telecommunications networks.

While the financial sector relies on this physical and virtual infrastructure to operate, it also depends on continued public confidence and involvement, without which normal operations would cease. This is a result of the fact that financial institutions maintain only a small fraction of their assets in cash on hand. During an emergency, if depositors and customers tried to withdraw their assets simultaneously, the system would experience severe pressures due to lack of funds. While federal safeguards are in place to prevent liquidity shortfalls, public confidence and participation in the financial sector are extremely important. Given that the financial sector plays such an important role in our economy and society, its security is imperative and it should be considered no less critical than other areas of infrastructure.

### **Chemical Sector**

The chemical sector is one of the most important in our country. It is responsible for a variety of everyday necessities and life-saving products. The chemical sector produces or contributes to the production of everything from critical drugs to clean drinking water to communications components and computer parts. Indeed, the chemical sector is integral to our way of life and is a large part of our national security and homeland defense efforts.

The chemical sector is a critical national asset and a \$450 billion business that makes the following contributions to our economy:

- directly employs more than 1 million Americans
- accounts for more than 5 million additional jobs in related industries such as agriculture, pharmaceutical, automotive and other industries
- contributes \$97 billion in products to the health care sector alone
- is the top U.S. exporting sector, accounting for 10 cents of every dollar in exports<sup>31</sup>

The sector itself is highly diverse in terms of company sizes and geographic dispersion. Its product and service-delivery system depends on many components, including raw materials, research facilities, manufacturing plants and processes, distribution systems, and supporting infrastructure services such as transportation and electricity.

The chemical sector not only provides products that are essential to our standard of living, it also manufactures products that are fundamental inputs to other commercial and industrial sectors, including the following:

- agriculture – fertilizer
- water purification – chlorine
- health care – polymers used in medical devices, PVC tubes for blood transfusions and needle kits, polycarbonate used in kidney dialysis filters

<sup>30</sup>ibid.

<sup>31</sup>“Chemical Security in an Age of Terrorism,” The CIP Report, vol. I (November 2002): 11.

- housing – pipes and shingles, siding, windows, electrical wiring, paints and insulation
- transformation – seat cushions, hoses and belts, airbags, tires, dashboards and seat belts
- communications – computer chips
- household and industrial products

Our food, water supply, clothing, housing, health care products and many other components of everyday life depend upon chemicals. This sector's importance to our economic security and daily lives makes it a very attractive target for terrorists. In addition to the economic consequences of a successful attack on the chemical sector, there is also the potential harm to public health and safety due to the fact that many large chemical facilities are near densely populated areas. Therefore, protecting this sector is a dual necessity, for our economic and everyday well-being as well as for public health and the environment.



## Chapter Two



What must you consider when making critical infrastructure policy?

## What are the challenges to protecting the various infrastructures?

### The New Reality

The technological sophistication of our society and institutions presents terrorists with many potential targets. Due to the relative newness of the concept of critical infrastructure protection, much of the expertise required to plan for and ensure the protection of critical infrastructures lies outside the federal government, including much of the knowledge about what needs to be protected. In effect, responsibility for defending our critical infrastructures is shifted down to the state and local governments and private sector stakeholders that make up the various infrastructure sectors. Therefore, when formulating policies, state leaders need to be aware of the challenges associated with securing each sector.

### Agriculture and Food Sector Challenges

The greatest challenges in securing our agricultural and food systems stem from the basic need for food and the extremely high sensitivity of the general public to food safety. These facts require food safety to be a high priority for states. The greatest threats to the food and agricultural systems are disease and contamination; however this sector's decentralized nature increases the challenge of assuring protection.

The existing system of federal, state and local public health and agriculture laboratories was established to detect the presence of traditional pathogens that sometimes contaminate foods. Although the system continues to guard against these pathological agents, the possible introduction of new or even engineered agents poses a future threat and challenge to state and local agencies, which may not have the resources, equipment or specialized expertise of corresponding federal agencies. However, because of the numerous points of entry to the nation's food system, detection is a critical tool to securing these sectors.

Processing crops, animals and other foodstuffs requires their transportation over long distances. During this process, these resources are stored in facilities where they may come in contact with other products. One challenge for states is to ensure that transportation system owners and operators, particularly those who deal with trucks and containers, implement the necessary safety and security standards to protect food products. In addition, officials need to be able to track the movement of animals and commodities to determine where an outbreak or contamination originates.

Unfortunately, there are serious institutional barriers and disincentives to cooperate and share information with state and local governments in the agricultural and food sectors. For the private sector, there are significant, direct economic disincentives associated with reporting problems or suspected contamination of foodstuffs. In addition, the market for these products is highly competitive. As a result, in order to prevent the financial consequences of what could be a false alarm, some companies may withhold information related to incidents involving suspected contamination.

For example, suppose a large supply of ketchup is contaminated. Almost all of the ketchup consumed in the United States is basically produced in two places in North America. These two facilities produce enormous amounts of ketchup each day. If a large supply of ketchup at one of these facilities was contaminated, the effect would be felt throughout the country. Where does the supply chain end for a product as simple as ketchup? It is distributed by numerous wholesale suppliers, sold by millions of retailers and used in millions of restaurants and homes. A disruption in supply or distribution of tainted ketchup could have devastating consequences for vendors and for the ketchup-consuming public. Would some companies go so far as to withhold disclosing where their ketchup came from in order to forego the financial consequences? States would be responsible for communicating effectively with the general public and for making sure that health officials acted to ensure that this contami-

---

Much of the expertise required to plan for and ensure the protection of critical infrastructures lies outside the federal government, including much of the knowledge about what needs to be protected. Therefore, when formulating policies, state leaders need to be aware of the challenges associated with securing each sector.

---

### Quick Facts on U.S. Critical Infrastructure

- Approximately 85% of U.S. infrastructure is privately owned and operated
- 1,912,000+ farms
- 75,000+ state and locally owned dams and reservoirs
- 1,800 federal reservoirs
- 700,000+ miles of drinking water networks
- 170,000+ public drinking water facilities
- 16,000+ publicly owned wastewater treatment facilities
- 5,800+ registered hospitals
- Emergency services/law enforcement organizations in over 87,000 U.S. localities
- 2 billion+ miles of telecommunications cables
- 160,000+ miles of electricity transmission lines
- 2,800+ power plants
- 104 commercial nuclear power plants
- 880,000+ oil wells
- 161 oil refineries
- 220,000+ miles of oil pipeline
- 300,000+ producing natural gas wells
- 1.3+ million miles of natural gas pipelines
- 4,000 offshore platforms
- 600+ natural gas processing plants
- 3.9 million miles of streets, roads and highways
- 100,000+ miles of rail
- Approximately 600,000 bridges
- 361 U.S. ports
- 500 train stations
- 5,000+ public airports
- 66,000+ chemical plants

nated supply was taken off the market. They would also need to cooperate and coordinate with neighboring states and the federal government. There are many other examples where a simple product such as ketchup could be used as a vehicle to attack the public.

Whether deliberately fomented by terrorists or not, contaminations and catastrophic attacks or events can harm people and animals and threaten to inflict pain or even death, along with substantial economic damage. Therefore, one of the greatest challenges states face is to ensure the timely reporting of information to allow for prompt decision-making and action. The fear of a negative public response and ensuing economic implications may influence the level of response taken by the agricultural and food sectors. States are at the forefront of this challenge, because public response to incidents will rely on the extent to and success with which state and local governments communicate with media outlets.

### Water Sector Challenges

The basic and undeniable human need for water is the driving factor for water infrastructure protection. While public perception regarding the safety of our water supply is also important, as is the safety of people who live or work near water facilities, the 170,000 public water systems must be the primary focus of critical infrastructure protection efforts. However, protecting the diverse and distributed water sector is one of the most difficult challenges for the states.

A small number of drinking water and wastewater utilities, approximately 15 percent of the systems, serve more than 75 percent of the U.S. population.<sup>32</sup> These massive water systems, located primarily in large urban areas, represent perhaps the greatest targets for terrorist attacks. While the smaller systems that serve fewer people are less likely to be perceived as key targets by terrorists or others who might seek to disrupt water infrastructure systems, these more numerous smaller systems also tend to be less protected, and thus may be more vulnerable to attack. This provides a great challenge to states because these systems tend to be located in areas or municipalities where additional resources are not available to extensively secure water infrastructure. Therefore, responsibility in the end ultimately lies in the hands of state government.

A successful attack or disruption, even at a smaller, local water system, could cause widespread panic, economic impacts, and a loss of public confidence in water systems nationwide. States must be wary of local threats that could result in physical destruction or disruption of the following systems:

- operating or distribution system components
- power or telecommunications systems
- electronic control systems
- reservoirs and pumping stations

Because of the structure and nature of the water sector, approaches to security and emergency response at water facilities are implemented at the state and local levels. The challenge for states is to expand beyond traditional concern for the structural condition of our water infrastructure to focus on disaster prevention and sustaining service in an emergency.

What would happen if a terrorist were to contaminate or gain control of an area's water supply? Such an instance occurred in Queensland, Australia in 2000. The local wastewater system had been leaking thousands of gallons of sludge into the waterways. It was eventually discovered that a man had used a computer stolen from the local water authority and a radio transmitter to gain control of the water system. (The man turned out to be a water consultant attempting to land a contract to fix the problem.) He had gained control of the

<sup>32</sup>Congressional Research Service, Terrorism and Security Issues Facing the Water Infrastructure Sector, 2.

SCADA (supervisory control and data acquisition) systems by remote, allowing him to control the release and flow of water and wastewater in the local system. He caused a large amount of damage and contamination by releasing wastewater into the waterways. While the consultant did have some insider knowledge of the water industry and the local water systems, he used standard, off-the-shelf software that anyone could obtain and he faced no obstacles once he infiltrated the system. States must be aware that similar systems are employed here in the United States and the same potential for disruption exists.

The nation's water resources are vital to our health and economic well-being. Therefore, states must face the challenges related to preventing and detecting terrorism against the variety of water systems by hardening facilities and providing backup support.

### **Public Health and Emergency Services Sector Challenges**

States face many challenges when considering how best to harden the public health and emergency services sectors against disruption or attack. Workers in these sectors continually place themselves in harm's way, in physically dangerous situations or in the presence of deadly communicable diseases, during all types of emergencies. Although danger is a routine part of their work, they must also be made aware that they could be targets of terrorism. States face the challenge of ensuring that public health and emergency service workers at the state, regional and local levels are supplied with both the perspective and the tools necessary to operate effectively in such situations.

The threats of bioterrorism and emerging infectious diseases, both natural and engineered, have been elevated to high priorities in the public health sector. Therefore, maintaining this infrastructure is vitally important to states. Since the ability to detect, contain and prevent infection has its strongest focus at the state level, detecting potentially contaminated individuals must be a priority. This is the greatest challenge states face with regard to the public health sector, because a new or unusual disease would most likely first be recognized through public health surveillance at the state or local level.

In addition, there are security challenges related to the ability of various segments of the public health sector to deliver critical services during a crisis. Many hospitals and other health facilities operate with limited profit margins and therefore have difficulty investing in security. States must be aware of the funding challenges these facilities face, whether they are in rural or urban areas. Additional public health sector challenges relate to the maintenance, protection and distribution of various stockpiles of resources needed during emergencies. States must be constantly aware that there are limited resources for rotating and replenishing supplies of critical materials and medicines.

States also need to be aware of the potential for terrorists to target prescription drug supplies by introducing counterfeit prescription drugs into the U.S. market. The Food and Drug Administration reports a 400 percent increase in the number of counterfeit drug cases in the United States since 1990. In fact, terrorists have already turned to using profits from counterfeit drugs to fund their operations. The Irish Republican Army did this in 1990 and as did the Middle Eastern terrorist group Hezbollah recently. If these groups are willing to use this method to obtain funds, it is logical to assume they would use it to attack the United States.<sup>33</sup>

If counterfeit versions of important drugs were introduced into the United States, a rapid response would be required not only by the federal government but also by states. This response would include communicating and coordinating with numerous health facilities, hospitals and drug distributors and tracking shipments of drugs. It could possibly even require difficult steps such as temporarily shutting down distribution chains. Counterfeit drugs could be introduced through fake Internet offers from outside the United States or by slipping them into the supply through smaller wholesale operations. These possibilities

---

**Since the ability to detect, contain and prevent infection has its strongest focus at the state level, detecting potentially contaminated individuals must be a priority.**

---



---

**States also need to be aware of the potential for terrorists to target prescription drug supplies by introducing counterfeit prescription drugs into the U.S. market.**

---

<sup>33</sup>Julie Appleby, "U.S. Drug Supply a Terrorism Target?" USA Today, 25 September 2003.

---

**Many critical state functions are tied to information technology, such as making payments to welfare recipients or state employees, supporting law enforcement with communications systems or electronic access to networks and criminal records, and operating state-owned utility and transportation services.**

---

require states and the federal government to think about protecting the U.S. drug supply, which is a critical component of the public health sector, and how technology could help prevent such occurrences.

The public health and emergency sectors face a common challenge: the sharing of information. It is vital that information-sharing capabilities are a top priority for both of these sectors. The public health sector already has a fairly developed infrastructure for addressing issues related to sharing of information, which is necessary when tracking, treating and curing diseases. But to deal with the threats of bioterrorism and new diseases, the ability to share and analyze information must be seamless and ongoing, and states must recognize that they have a huge role to play.

Lessons from September 11 highlighted inadequate information sharing among law enforcement and emergency first responders as a major challenge. The ability to share information, assess situations and coordinate efforts is critically important when responding to major disasters. Whether it is among jurisdictions, across multiple agencies or across levels of government, shortfalls in the ability to communicate and coordinate are a certain recipe for failure.

Although the existing infrastructure is sufficient for dealing with routine accidents and regional disasters, the September 11 attacks revealed shortfalls in emergency services' capacity to respond to large-scale terrorist incidents and other catastrophic disasters that require extensive cooperation among local, state and federal emergency response organizations. To prepare for future disasters, states need to be aware of telecommunications problems, such as incompatible systems; the challenges of enhancing protection through security to mitigate secondary attacks; and any existing weaknesses in systems that support emergency response personnel.

The communications systems of many state and local agencies have been developed and implemented with respect to unique needs. This often prevents interoperability and hinders emergency services' ability to communicate and coordinate resources during crises. Failure of communications systems during a crisis impedes the progress of response and may put additional lives at risk.

Our nation must be prepared for the possibility of major disasters and terrorist events. Readiness for such events means that our state and local public health and emergency services sectors must be able to rapidly identify, investigate and control the consequences of such events. Their response may make the difference between chaos, panic and mass casualties and a significant reduction in loss of human life and property.

### **Telecommunications/Information Systems Sector Challenges**

The telecommunications/information systems sector faces significant challenges to protect its vast and dispersed critical assets, both cyber and physical. Because the federal and state governments and many other critical infrastructure industries rely heavily on the public telecommunications infrastructure for vital services, protection initiatives are vitally important.

While all levels of government are working together to address the vulnerabilities of the telecommunications and information systems sector, state and local governments face special challenges related to working with the private sector to address vulnerabilities in the nation's computer-controlled systems, and to develop mechanisms and processes to protect them from attack. The private sector plays a central role in securing cyberspace, not only because it depends on this infrastructure to conduct business, but also because it owns and operates the vast majority of the infrastructures and cyber systems on which the nation depends.

Many critical state functions are tied to information technology, such as making payments to welfare recipients or state employees, supporting law enforcement with communications systems or electronic access to networks and criminal records, and operating state-owned utility and transportation services. Preventing disruption from physical or virtual (cyber)

attacks and responding quickly when they occur ensures that these systems continue to provide important services that the public needs and expects around the clock.

Information technology systems make state governments more efficient, responsive and accessible. But it is difficult for hundreds of government agencies to adopt common information technology architectures and management (audit) standards. In addition, many states do not have security-confidentiality laws. This inhibits information sharing about security breaches and unwelcome intrusions across branches of government and jurisdictions. Also, states do not have security risk assessments on all their critical information technology assets. This thwarts their ability to develop security plans and report on security performance. Finally, few states have a security portal to coordinate information technology and emergency management responses across jurisdictional boundaries. States need to realize the challenges that arise from not being able to appropriately manage information technology assets, report on security performance, and share resources.

Many government systems provide essential services that touch citizens in a highly direct and personal way. These services are part of the nation's critical infrastructure, which makes information technology security a key aspect of homeland security. If attacks undermine the public's confidence in the integrity of these systems, then states will be unable to expand these services to reap the potential benefits.

Protecting the physical infrastructure of the telecommunications sector provides a challenge for states, as the industry continues to evolve due to technology advances, business and competitive pressures, and changes in the regulatory environment. While this sector must deal with traditional natural and human-based threats daily, such as weather and unintentional damage to cables, now it must also face the threat of sabotage by terrorists.

Key challenges for states will deal with local telecommunications carriers and issues of service reliability, security and effective risk management. States must continue to place a high priority on the consistent application of security across the infrastructure. The greatest challenge to states is that, although private- and public-sector stakeholders share similar objectives, they have different perspectives on what constitutes acceptable risk and how to achieve security and reliability. Agreements have remained elusive and states will have to recognize the challenge that lies in working with the private sector to reach a sustainable security threshold and acceptable security requirements.

An added difficulty lies in the growing interdependence among the various critical infrastructures, which means that a direct or indirect attack on any one of them could result in cascading effects across the others. This is especially true with respect to physical telecommunications structures, which provide the backbone of our economic and national security. Therefore, it is vital that state governments and industry work together to secure the telecommunications infrastructure. States will have to take the lead on this effort, as the recent economic downturn has forced companies to spend their resources on basic network operations rather than on securing and enhancing infrastructure. This weakness threatens to amplify the financial impact of damage to physical information technology infrastructure.

The greatest challenge in preventing disruption to the telecommunications and information systems sector is protecting it from new computer viruses. In today's global society, almost everything is connected to some sort of computer system. While this level of connectivity allows us to accomplish tasks much more effectively than we could in the past, it also makes us more vulnerable. The "I love you" virus of May 2000, for example, showed how this vulnerability can be exploited. First detected in Asia, the virus quickly swept around the world in a wave of indiscriminate attacks on government and private sector networks, infecting nearly 60 million computers and causing billions of dollars in damage.

The risks associated with our nation's reliance on interconnected computer and telecommunications systems are substantial and varied. States must be aware of these risks and the challenges associated with securing this important infrastructure, because failure to do so

**A catastrophic event that halted energy supplies could mean severe economic disruptions in the transportation sector, manufacturing, information technology systems, the distribution and marketing of goods and many other sectors.**

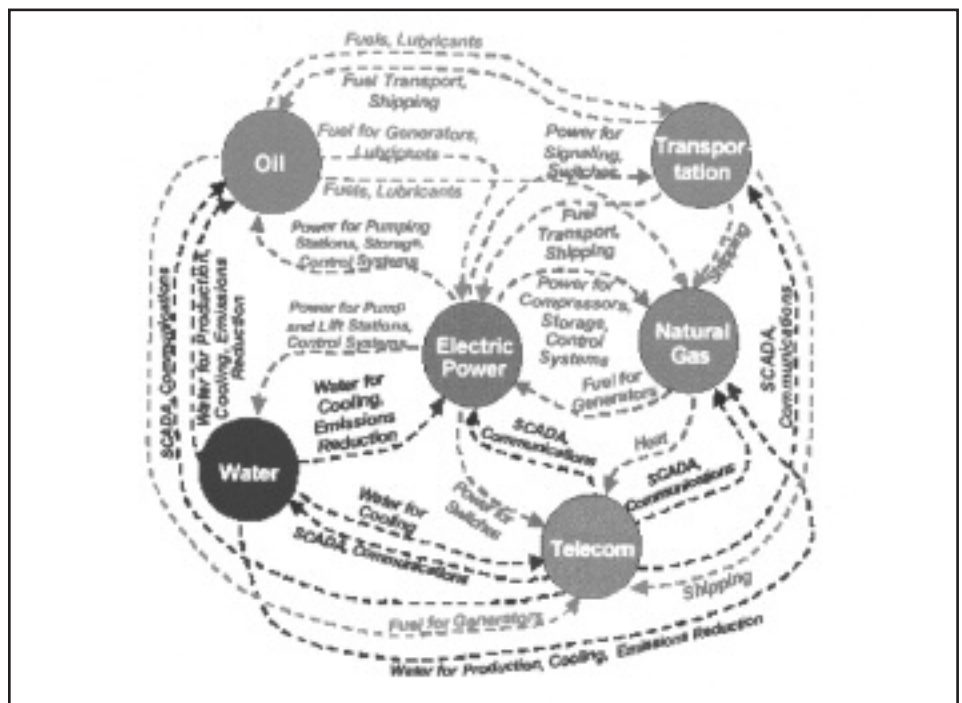
could endanger the nation's economic and physical security.

### Energy Sector Challenges

Whether from natural disaster, equipment failure or terrorist attack, our energy sector faces a broad array of risks. The events of September 11 increased our awareness of these risks. Such threats are amplified by the interconnected nature of our energy systems. From pipelines to wellheads, nuclear plants, the electric grid, storage facilities and distribution facilities, our energy infrastructure is to some degree vulnerable and this poses numerous challenges.

The U.S. energy systems are central to our way of life and are integral to our nation's other infrastructures. What infrastructure doesn't rely on energy? Figure 2 illustrates the interconnected nature of energy and other infrastructures. An attack or disaster that disrupted or destroyed our energy sector would have major impacts throughout society, including economic disruptions, environmental effects and impacts on public health and safety.

**Figure 2: Interdependence of Energy and Other Critical Infrastructures**



Source: Jim Peerenboom, Argonne National Laboratory, 2002.

A reliable energy system is the backbone of our national economy. A catastrophic event that halted energy supplies could mean severe economic disruptions in the transportation sector, manufacturing, information technology systems, the distribution and marketing of goods and many other sectors. California's power grid crisis of 2000-2001, for example, cost businesses millions of dollars as the outages and rolling blackouts disrupted daily economic activity. Energy disruptions inflict economic losses due to equipment damage, material loss, data loss, costs of running backup generation and productivity losses due to outages.

Energy disruptions or attacks on energy infrastructure could also pose environmental threats. Attacks on oil wells or tankers could cause spills or oil slicks that could harm shorelines, waterways and landscapes. A security breach or attack on a nuclear facility could render significant areas surrounding the facility uninhabitable due to radiation contamination. In addition, while not as damaging as some other consequences, disruptions to major power

plants or transmission facilities could force electric suppliers to rely on less efficient, backup generation units that emit much more pollution into the atmosphere.

Disruptions to our energy systems could also affect public health. As mentioned above, an incident at a nuclear facility would not only affect the environment, but could also cause significant radiation sickness or poisoning among local populations. Interruptions in power supply to hospitals could affect patients' health. Loss of power to water or sewer systems could result in poor water quality and could affect public health. Power disruption could have cascading effects, causing fires, additional release of radiation or hazardous materials, and transportation gridlock, resulting in numerous accidents. The possible effects are numerous. Therefore, the security and resilience of our energy systems is of major importance to our society.

### Electricity Challenges

The electricity sector is highly complex with a vast network of systems that extend throughout the country and into other parts of North America. Many of the sector's key assets, such as generation facilities, key substations and transmission systems, present unique security challenges.

The complexity of the country's power system makes protection especially challenging. While increased system integration has provided system redundancy and improved efficiency, it has made the system more complicated and harder to operate. Therefore, when faced with disruption, systems may be less likely to respond.

Another challenge is the electricity sector's growing dependence on Internet communications. Without the ability to transfer data among control centers, receive signals from remote equipment sensors and interpret vast amounts of data, these systems could not operate. However, because of the Internet's vulnerabilities, power systems' command, control and communications are at a greater risk of disruption.

Increased competition and market forces within the energy sector are affecting energy security. Many energy companies have experienced economic difficulties and bankruptcy due to market pressures exerted by the collapse of Enron. This has altered their perspectives toward security and their responsibilities. While the stakeholders in the energy sector are diverse in size, capabilities and focus, individual companies pay for levels of protection that are consistent with their resources and customer expectations. While these companies may seek to recover the costs of new security investments through proposed rate or price increases, states traditionally regulate their ability to do so. Under current federal law, there is no assurance that the electric industry would be allowed to recover the costs of mandated security measures through rate increases. States need to work with the industry to address this issue in order to ensure reliability and security in the electricity sector.

### Nuclear Power Plant Challenges

While the loss of a nuclear plant would not have a significant impact on the security or resilience of the energy grid, an attack or catastrophic event at a nuclear facility could produce disastrous results. The release of radioactive material from such an event could cause sickness and death and could leave a large area uninhabitable for a significant period of time. Even if radioactive material were not released in the aftermath of an event, public misconceptions or misunderstandings of the potential consequences could have a significant negative impact. Therefore, the security of these facilities is paramount.

Although the Nuclear Regulatory Commission oversees all safety issues related to nuclear plants, state and local governments do have input into NRC decisions and hearings. In addition, since any potential emergency would require a local response, states must work with

---

**While the stakeholders in the energy sector are diverse in size, capabilities and focus, individual companies pay for levels of protection that are consistent with their resources and customer expectations.**

---

**Perhaps the most challenging factor in protecting oil and natural gas facilities is their wide geographic distribution.**

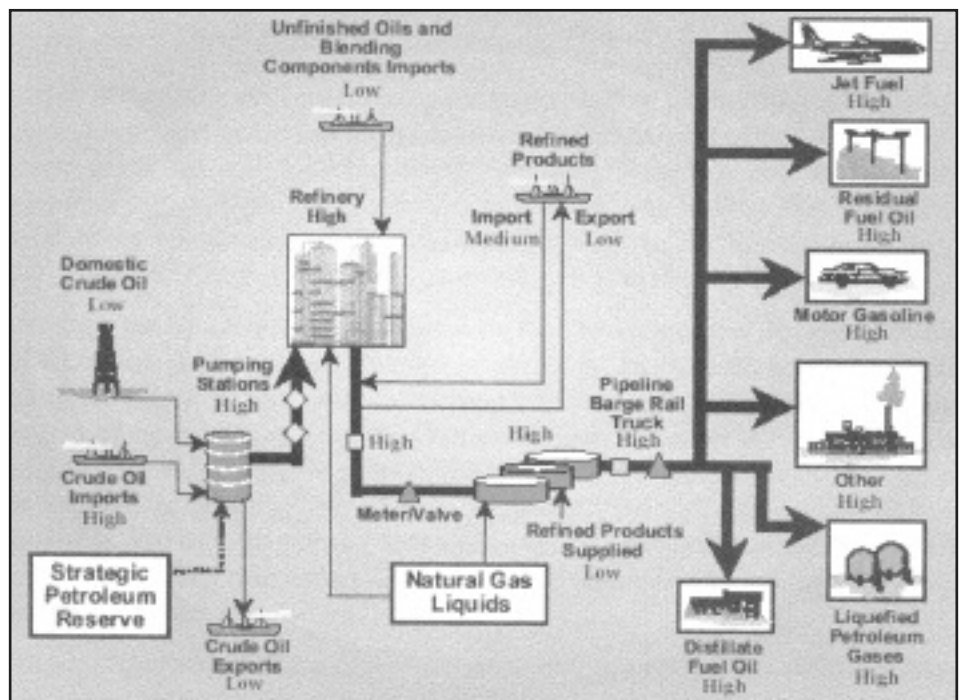
the federal government and industry participants to address safety needs and responses.

While the NRC continuously monitors, examines and conducts threat and vulnerability analysis for nuclear power plants to identify additional security enhancements that may be needed, states must continue to work with the NRC, the federal government and the industry to draft off-site emergency response plans to ensure additional measures are enacted and actions are taken to strengthen nuclear facilities.

### Oil and Natural Gas Sector Challenges

Perhaps the most challenging factor in protecting oil and natural gas facilities is their wide geographic distribution. This characteristic puts both sectors at risk due to the numerous vulnerabilities that exist from production to distribution. Different parts of each system for oil and natural gas are subject to different threats depending on whether assets, products and facilities are geographically concentrated or isolated. **Figures 3 and 4** below indicate the different levels of vulnerability that exist in each sector from production to delivery.

**Figure 3: Vulnerability of Oil Sector from Production to Delivery**

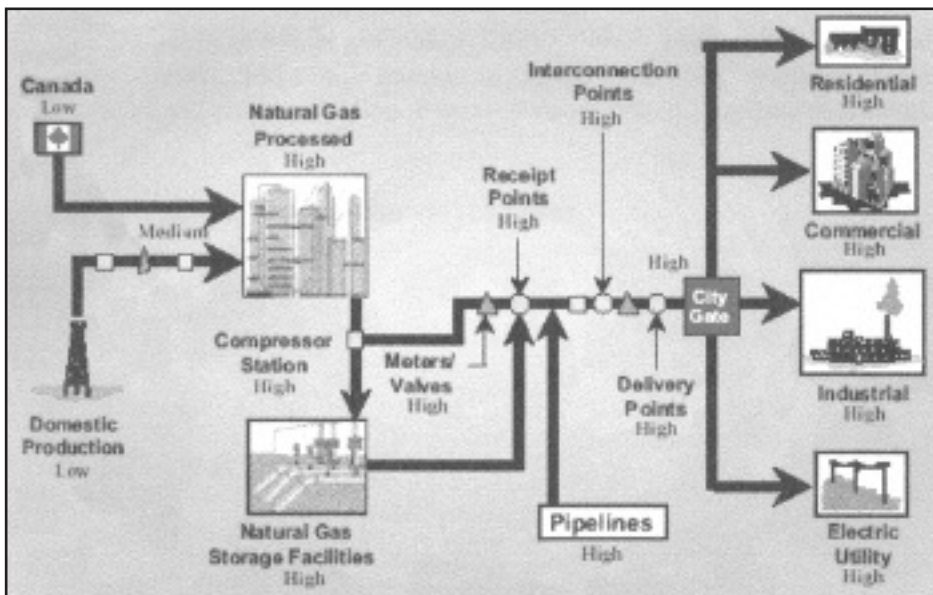


Source: National Petroleum Council, 2002.

For the oil network, the level of vulnerability varies throughout the production and distribution chain, ranging from moderate to high as depicted in Figure 3. The network's vast distribution chain and decentralized nature make it difficult to secure. In addition, petroleum products are an environmental and public health threat at almost any stage, whether in storage, transportation or distribution.

For the natural gas network, vulnerability increases in the transportation, storage and delivery stages, partly due to the vast distribution and decentralized nature of the network at this point, which makes it harder to secure. In addition, natural gas is transported and stored in a compressed state, which makes it more vulnerable and combustible. The transportation, storage and delivery components of the natural gas network are located throughout the country in all states. The threat is not only to public health but also to the economy.

**Figure 4: Vulnerability of Natural Gas Sector from Production to Delivery**



Source: National Petroleum Council, 2002.

Certainly, the protection effort is aided by the presence of the Strategic Petroleum Reserve (SPR), which is often considered the nation's first line of defense against disruptions in petroleum supplies. This emergency supply of crude oil is stored in huge underground salt caverns along the coastline of the Gulf of Mexico. The reserve significantly reduces our nation's vulnerability to the adverse economic and security threats of supply interruptions. However, as the largest emergency supply of oil in the world – more than 600 million barrels with a value of more than \$20 billion – its size and value make it vulnerable to attack as well. Therefore, states cannot necessarily rely upon the SPR to relieve them of the pressure of working to secure their energy infrastructure.

The physical infrastructure of the oil and natural gas sectors has remained largely the same over time, consisting of wells, gathering systems, processing facilities and transmission and distribution systems. The way the sector does business, however, has changed greatly due to the use of electronic control systems. Operating processes, from producing fields to refineries and pipelines to the sale of raw materials, depend today on electronic systems. Therefore, the energy sector is vulnerable not only to physical attacks and events, but also to virtual threats and disruptions to the telecommunications and information networks.

The energy industry faces significant barriers to carrying out protection responsibilities. Nearly all energy companies have seen their profits and value drop since 2000. Many companies consider the financial burden of implementing risk assessments and security upgrades too great to bear. This is compounded by the decentralized nature of the oil and gas sectors, which are characterized by a wide distribution of asset ownership. Many thousands of owners and operators, with differing asset portfolios, operate independently of one another. This diversity, however, provides an advantage. A single attack is not disastrous to all, and an isolated incident at a single facility probably would not affect large numbers of users for prolonged periods.

Fortunately, due to public-safety requirements that have been in place for some time, the oil and natural gas sectors already have substantial protection programs in place. However, states should be aware that any deference of risk in effect transfers some of that risk to state and local governments. Local police and fire departments will be the first responders to an attack or disaster that damages or destroys oil and natural gas facilities. Therefore, states need to help ensure that these responders are prepared to confront such situations.

---

**Public and private expenditures on transportation account for approximately 17 percent of the gross national product.**

---



---

**With approximately 3.9 million miles of roads, more than 100,000 miles of rail, nearly 600,000 bridges, more than 300 ports, approximately 2.2 million miles of pipelines, 500 train stations, and more than 5,000 public airports, the transportation system's decentralized nature and the vast number of components make it vulnerable.**

---

State officials must be aware that repairing damaged oil or natural gas infrastructure may be a slow process. During rebuilding, industries may face challenges due to local, state and federal construction permits or waivers; requirements for environmental reviews and impact statements; and lengthy processes for obtaining construction rights-of-way for the placement of pipelines. Therefore, states will have to work through their public service commissions and regulatory processes to partner with the industry to ensure quick restoration of services.

### **Transportation Challenges**

The U.S. transportation infrastructure is vital to our economic and national security. Public and private expenditures on transportation account for approximately 17 percent of the gross national product.<sup>34</sup> Americans depend on some form of transportation in nearly every aspect of daily life. Since disruption of our transportation systems could have a disastrous impact on the nation's economy and security, states need to be aware of the challenges behind securing the transportation sector.

Transportation stakeholders, states included, face numerous challenges in securing the nation's transportation system. While some of these challenges are common to all modes of transportation, others vary with specific modes, such as aviation, maritime or surface transportation. Maritime and land systems, for instance, are designed as open-access systems, allowing users to enter at multiple points. However, this openness leaves them vulnerable, because it is extremely difficult for operators to monitor or control who enters or leaves the systems.

While each sector has unique challenges, common themes include the extensiveness of our transportation systems, the number of stakeholders involved in transportation security, and the interconnectivity of the system.

The sheer size of the U.S. transportation system provides a substantial number of potential targets for terrorists and makes it difficult to secure. With approximately 3.9 million miles of roads, more than 100,000 miles of rail, nearly 600,000 bridges, more than 300 ports, approximately 2.2 million miles of pipelines, 500 train stations, and more than 5,000 public airports, the system's decentralized nature and the vast number of components make it vulnerable.

In addition, the large number of stakeholders, including more than 20 federal agencies, state and local governments, and a huge number of private companies, provides challenges related to coordination and communication. **Figure 5** illustrates this expansive network.

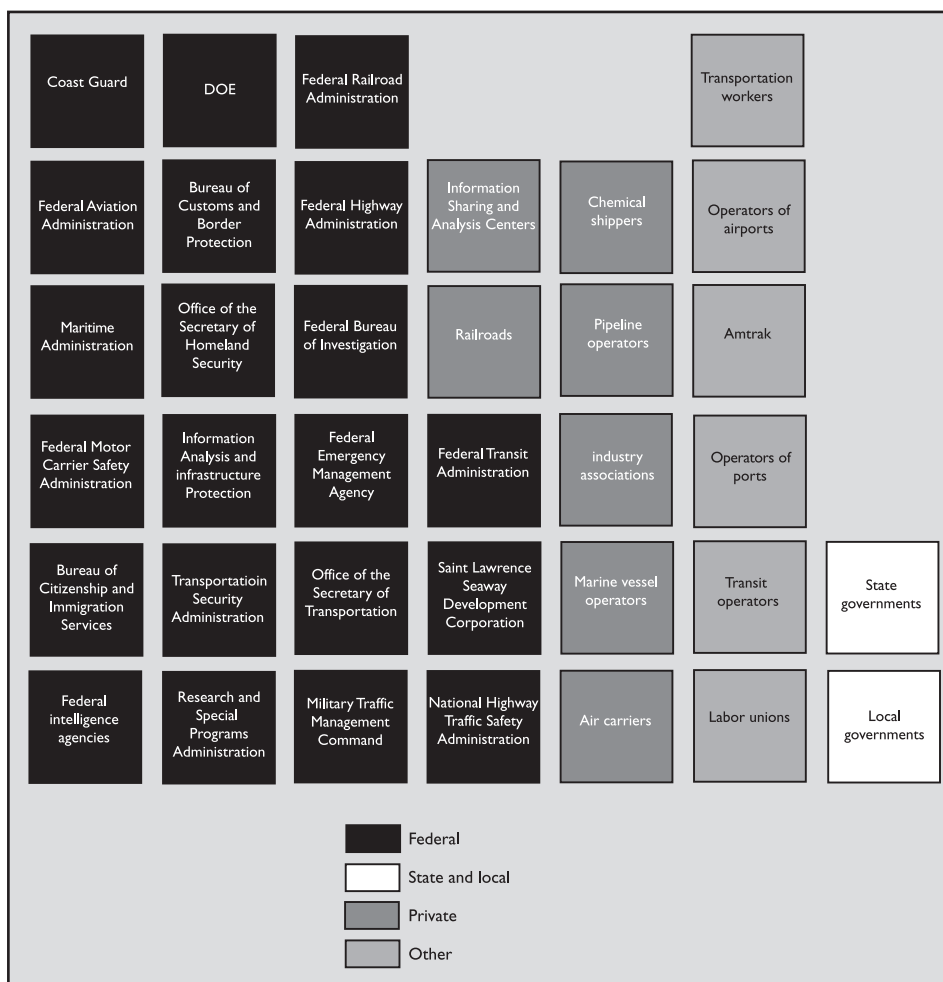
Approximately 2,000 pipeline companies and 571 railroad companies own and operate the pipeline and freight railroad systems. In addition, 83 passenger air carriers and 640,000 interstate motor coach and carrier companies operate in the United States.<sup>35</sup> However, state and local governments also own large portions of the nation's highways, transit systems, and airports, including more than 90 percent of the total mileage of highways.

State and local governments play a critical role in securing the system not only because they own a large portion of it, but also because they serve as first responders to incidents involving transportation assets. It is important for state and local governments to recognize the challenges in clarifying roles and coordinating efforts in such an expansive sector.

In addition, state and local governments administer and regulate many sectors of the transportation system and provide protective and emergency response services. And, although the federal government owns a limited share of the transportation system, it issues regulations, establishes policies, provides funding, and sets standards for the different modes of transportation.

<sup>34</sup>The CIP Report, vol. I (January 2003): I.

<sup>35</sup>Governmental Accounting Office, Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO-03-843, 30 June, 2003, 6.

**Figure 5. Transportation sector stakeholders**

Source: GAO.

The basic function of the nation's transportation systems, combined with their interconnected nature, creates many interdependencies between transportation and nearly every other sector. In short, a threat to the transportation sector may impact other industries that rely on it and vice versa. States must be constantly aware of the fact that so many other sectors rely on some sort of transportation.

Due to the susceptibility of transportation modes to attack by terrorists and their potential to be used as weapons of attack, as we saw on September 11, states must be prepared. Even in a time of tight budgets, vulnerabilities must be assessed, staff must be constantly trained and ready, and states must be prepared to respond to terrorism-related emergencies. Officials must keep in mind that, for the most part, these are new responsibilities for state transportation organizations. However, the price of not recognizing and addressing these challenges is our economic security and personal safety.

### Aviation Challenges

The aviation sector faces several unique protection challenges. Chief among these is its distributed nature and open-access design. The aviation network contains thousands of entry/exit points at home and abroad, making it difficult to secure. In addition, as September 11 showed, not only is the aviation sector a potential target, but it can also serve

---

State and local governments play a critical role in securing the system not only because they own a large portion of it, but also because they serve as first responders to incidents involving transportation assets.

---

as a potential weapon for terrorists.

Before September 11, the security of airports and their associated assets was the responsibility of private carriers and state and local airport owners and operators. However, following the attacks, Congress passed legislation establishing the Transportation Security Administration as the authority responsible for assuring aviation security. With this step, states were somewhat taken out of the loop with regard to securing aviation infrastructure. However, this does not mean unique protection challenges do not exist related to the aviation sector. As the national physical protection strategy outlined, these challenges include the following:

- **Volume** – Every day, the aviation sector transports millions of passengers and bags, as well as other cargo, making it difficult to secure planes and facilities.
- **Limited capabilities and available space** – The limited space in aviation facilities and the limited amount of detection equipment available impact security.
- **Time-sensitive cargo** – The fact of that a great deal of cargo is time-sensitive and essential for many businesses presents challenges in securing the aviation sector because lengthy processing and transportation times could negatively affect the U.S. economy.
- **Security versus convenience** – The process of limiting congestion and flight delays complicates security.
- **Accessibility** – The open nature of airports and the aviation system provides challenges in securing the system.<sup>36</sup>

### Surface Transportation Challenges – Highways, Trucking and Mass Transit

Surface transportation in the United States is an extraordinarily large, diverse and complex system responsible for the movement of vast quantities of passengers, freight and commodities via rail, road, pipeline and water. As discussed earlier, the system includes millions of miles of roads and pipelines, hundreds of thousands of bridges, thousands of airports, and hundreds of ports and train stations, as well as many thousands of independent, yet intertwined, operators and stakeholders. Some operators are large and some are small; some are public while others are private. The U.S. surface transportation system is highly decentralized. And, despite its regulatory and other responsibilities for transportation, the U.S. Department of Transportation actually owns or operates almost none of the nation's system. This fact makes addressing protection of surface transportation systems very challenging and highlights the fact that the majority of these systems are in the hands of state and local governments and private sector operators.

Traditionally, security has rarely been a high priority for the highway and trucking sectors. Unlike the aviation sector, which has seen a series of incidents since the 1960s that have brought security issues to the forefront, there has been little awareness of security in these sectors. Although many states have conducted risk assessments of their highway infrastructures, this has been done relative to age and service needs, not protection from attacks. Therefore, a thorough examination of protection challenges is difficult, although some challenges are apparent.

The size and vast operations of the highway, trucking and mass transit sectors provide advantages, making them more resilient, flexible and responsive to various conditions. These same characteristics, however, cause protection challenges. The decentralized nature of these sectors causes them to be fractionalized and regulated by multiple jurisdictions at state, federal and local levels. In addition, the sheer number of facilities and components makes securing them all impossible.

As a result of the diversity and widely distributed nature of these sectors, there is no coher-

<sup>36</sup>The White House, National Strategy for the Physical Protection of Critical Infrastructure, 55.

ent picture of risks or a set of security criteria on which to base protection planning. States should be aware of these issues and seek to work with the various stakeholders to ascertain what conditions constitute threats. One such threat is transportation choke-points (such as, bridges and tunnels, intermodal terminals, border crossings, and highway interchanges) that can present protection challenges because large numbers of people in these areas during peak times could make attractive targets.

An issue that further complicates protection of these sectors is the need to balance security concerns with accessibility, convenience and commercial activity needs. Security measures that limit these features risk impeding commercial activity in the trucking sector and driving riders away from transit systems. States must find ways to balance security with these other needs.

In addition, the openness of the trucking and transit sectors can make them potential targets; vehicle could be used as weapons. In the trucking sector, for example, more than 11.2 million trucks entered the United States in 2001. These vehicles and others already in the country have large cargo capacities, are highly mobile and offer easy access to key population centers.

Some people may blame the lack of security measures and coordinated efforts among stakeholders on insufficient government or private-sector funds. The truth, however, is that due to these sectors' vast size and scope of operations, many security measures are cost-prohibitive. For example, while transit authorities must have the financial resources to respond to emergencies and maintain adequate security levels, the cost of implementing new security requirements could result in significant financial consequences for the industry. In a recent GAO report, one transit agency estimated that an intrusion alarm and closed circuit television system for only one of its portals would cost more than \$250,000.<sup>37</sup>

Given the number of public and private owners and operators in both the truck and mass transit sectors, the cost of infrastructure protection is a major challenge – especially for small businesses. In addition to the cost of new security investments, trucking and mass transit organizations also regard the possibility of security-related delays as a potential problem of major financial significance.

Another challenge is the way in which sector security incidents are handled across multiple jurisdictions. Because different law enforcement agencies at different levels of government have different approaches to crimes involving trucking or mass transit, law enforcement responses to security incidents in this sector are inconsistent across jurisdictional lines. When considering protection policy in these areas, states should take these matters of coordination and jurisdiction into account.

Finally, as Figure 5 illustrated earlier, there are numerous stakeholders within these sectors and they are regulated by various agencies. These agencies must communicate and work together across various levels of government. For example, since mass transit is funded and managed at the local level and operates on a nonprofit basis, the Federal Transit Authority has limited authority in terms of security planning and oversight. So the burden falls upon state and local governments to create policy and to respond to disasters and attacks.

State and local governments, the private sector and the federal government all have roles and responsibilities in securing these sectors. State officials need to understand the structure of responsibility and regulatory authority within their states and with respect to the federal government in order to facilitate coordination when formulating policy.

## Maritime Mode Challenges

The size, diversity, scope and complexity of the maritime shipping infrastructure make the

<sup>37</sup>Governmental Accounting Office, Mass Transit: Challenges in Securing Transit Systems, GAO-02-1075T, 18 September, 2002, 2.

---

**Given the number of public and private owners and operators in both the truck and mass transit sectors, the cost of infrastructure protection is a major challenge – especially for small businesses.**

---

---

**States need to focus protection efforts on pipelines that significantly impact the economy as a whole, such as those that serve the energy industry.**

---

inspection of all vessels and cargo that enter our ports, and the protection of these ports, an extremely difficult undertaking. More than 17,000 containers enter U.S. ports by ship daily. However, only about two of every 100 containers are actually checked or searched by customs agents.<sup>38</sup>

Among the foremost challenges for states are the industry's diverse nature and the multiple jurisdictions under which it operates. State and local governments control some port facilities, while private corporations own and operate others. Many ships are privately owned and operated. Major portions of the maritime industry's operations, however, are international in nature and are governed by international agreements and multinational authorities, such as the International Maritime Organization. In addition, negotiation of maritime rules and practices with foreign governments is the responsibility of the federal government and the State Department. Therefore, efforts to increase the security of the maritime industry and certain ports must also consider these issues of multiagency jurisdictions and the corresponding international framework of the industry.

### **Pipeline Mode Challenges**

Perhaps the first main challenge to thinking about pipeline protection issues is to recognize that there are several hundred thousand miles of pipeline spanning the country, carrying everything from combustible natural gas, oil and gasoline to drinking water. It is unrealistic to expect every inch of these pipes to be secured. Therefore, states need to focus protection efforts on pipelines that significantly impact the economy as a whole, such as those that serve the energy industry. Nevertheless, many of the products that pipelines deliver are volatile and many of the pipelines themselves run through or into major population centers. Therefore, their protection is a significant issue.

The pipeline industry must determine what to protect and when to protect it, balancing infrastructure protection with the need to maintain cost-effective operations. For example, during holiday or high travel summer months, gasoline pipelines operate at peak capacity and are extremely important to most of the country. During the winter months, natural gas is in high demand due to home heating. Natural gas pipeline systems during this time typically operate at peak capacity and any serious disruption could have a tremendous effect not only on natural gas prices and our economy, but also on public health. Therefore, it is extremely necessary for state officials to recognize that pipeline networks are not independent entities, but are vital parts of industrial and public service networks. Loss of a pipeline or a network of pipelines could impact many people who depend on the commodities these networks deliver.

Another challenge is that many pipelines cross numerous state, local and even international jurisdictions (Mexico and Canada). The number of stakeholders creates multiple regulations and security factors that can be confusing and sometimes even conflict. Dealing with multiple jurisdictions can also affect operators' actions during a disruption and can impede their ability to quickly re-establish service. In addition, the pipeline industry, energy and telecommunications sectors are all very interdependent, which necessitates cooperation with these other critical infrastructures during protection and response planning and may require additional coordination efforts at the state and local levels.

Individual companies have difficulty assessing the broader implications of an attack on their critical facilities. These interdependencies call for cross-sector coordination in order to be truly responsive to national concerns. Additionally, some issues concerning recovery or reconstitution will require at least regional planning within the industry, as well as the sharing of sensitive business information, which may create proprietary concerns.

While the vast expanse of the nation's pipeline network creates significant challenges, it

<sup>38</sup>Kerry E. Julian, "Trucking Security: Managing freight movement in a new era," *Professional Safety*, vol. 48 (April 2003): 20.

also creates an advantage in that most elements of pipeline infrastructures can be quickly repaired or bypassed to mitigate disruptions. Therefore, destruction of one or even several key components would not disrupt the entire system. This makes the pipeline industry's ability to respond to and recover from disasters and disruptions better than that of other infrastructure sectors.

### Rail Challenges

Like the pipeline system, the nation's railway system is vast and complex, and like the maritime sector, it provides multiple points of entry into the United States. The size and scope of the rail sector make it difficult to react to and guard against threats, complicating protection efforts for states.

In addition, hazardous materials are often transported by rail, which poses risks to populated areas through which trains pass, as well as to state emergency workers and first responders. While these materials are often essential to other sectors or businesses, the potential for disaster is great. Therefore, states must always ensure they are part of the decision-making process regarding hazardous material transport and work to coordinate with industry and other levels of government.

However, while trains can make attractive targets, the rail sector does possess an advantage in that trains can be confined to specific, controllable routes. If a threat is detected, they can be diverted off of mainlines or routes that would put them near population centers. In addition, the potential for national-level disruptions within the rail sector is limited because rail traffic can be diverted or other forms of transport can be used.

States should also be aware that the rail sector is not uniform, and therefore protection solutions cannot be applied uniformly across the sector. Differences in design, structure and purpose of railway stations complicate the sector's overall protection framework. Any protection efforts that do not take this into consideration risk stifling commerce to meet security needs – simply swapping one consequence of a security threat for another. The highly competitive rail industry has already faced additional security costs during periods of heightened alert since September 11. States must be aware of the costs to industry of additional security measures and must look for security solutions that allow commerce to continue to flow.

### Banking and Finance Sector Challenges

According to the Federal Reserve Board, U.S. financial institutions held more than \$23.5 trillion in assets as of the second quarter of 2002 – a \$2 trillion increase from the first quarter of 2001. Without question, it is easy to understand why this sector is important to the states. Besides the fact that it facilitates commerce and allows our economy to function, the banking and finance sector employs numerous people in every state, facilitates the operation of state economies and governments and provides services without which government and society simply could not function.

Of course, several federal entities play the main roles, partnering with the private sector, to protect the financial services industry's critical infrastructures and ensure its future operations. States are also involved in this equation, not only as regulators, but also on behalf of their residents. Therefore, it is important that they understand the challenges in addressing the vulnerabilities of the financial services sector.

The banking and financial services sectors face two main threats in terms of infrastructure protection. Like other critical infrastructure sectors, they face cyber-based threats (attacks from individuals and groups engaged in espionage, terrorism or criminal activity). They also face indirect threats from being dependent on other critical infrastructures. For example, major disruptions in telecommunications or power infrastructure could directly affect the banking and financial services sectors.

---

**States should also be aware that the rail sector is not uniform, and therefore protection solutions cannot be applied uniformly across the sector.**

---



---

**The banking and financial services sectors face two main threats, those that are cyber-based and those that arise from being dependent on other critical infrastructures, such as the telecommunications and energy sectors.**

---

The financial services and banking sectors use computer networks for many different applications, including customer service, online banking, money transfers, securities trading and business operations. As these networks have increased the degree to which these sectors rely on the Internet, they have made these systems more accessible from the outside. This reliance on the Internet and increased accessibility pose significant information security risks if vulnerabilities are left unsecured.

However, overall, the potential for monetary gains and economic disruptions is the main factor that makes these sectors attractive targets. State officials should be aware that the main challenge in times of crisis or disaster is maintaining public confidence in our financial institutions and ensuring that financial institutions, financial markets and payment systems can meet the demands placed on them in order to remain operational or to quickly restore operations in the event of disruption. To that end, the Department of the Treasury and federal and state regulatory communities have emergency communications plans for the banking and finance sector.

### Chemical Sector Challenges

The chemical sector and its products are vital to a variety of applications and other infrastructure sectors. Not only could the disruption of this industry threaten our economy and way of life, but an attack or accident resulting in a large release of chemicals could contaminate the environment, which could affect public health. Therefore, chemical facilities may be attractive targets for terrorists intent on causing economic harm or loss of life.

The risk of an attack varies among facilities, depending upon the location and the types of chemicals they store or manufacture. Many facilities are located in populated areas, where a chemical release could result in injuries or death. No specific data exist on the actual effects of a successful terrorist attack on chemical facilities. But, according to the Environmental Protection Agency, 123 chemical facilities located throughout the nation have the potential to produce a toxic “worst-case” scenario in which more than 1 million people residing in the surrounding area would be at risk of exposure to a cloud of toxic gas if a release occurred. Also, approximately 700 facilities could each potentially threaten at least 100,000 people in their surrounding areas while more than 3,000 facilities could each potentially threaten more than 10,000 people (See Figure 6).<sup>39</sup>

Figure only includes those facilities where an accident could result in a “worst-case” scenario, not to include facilities that only have flammable chemicals, since flammable chemicals travel shorter distances and would therefore affect less people.

In addition, the federal government has identified 140 toxic and flammable chemicals that, if released into the air in sufficient amounts, would pose the greatest risk to human health and the environment. Including other industries that use chemicals as inputs into their processes and must store them for periods of time, the federal government estimates that more than 15,000 facilities in the United States produce, use or store more than threshold amounts of these 140 hazardous chemicals.<sup>40</sup>

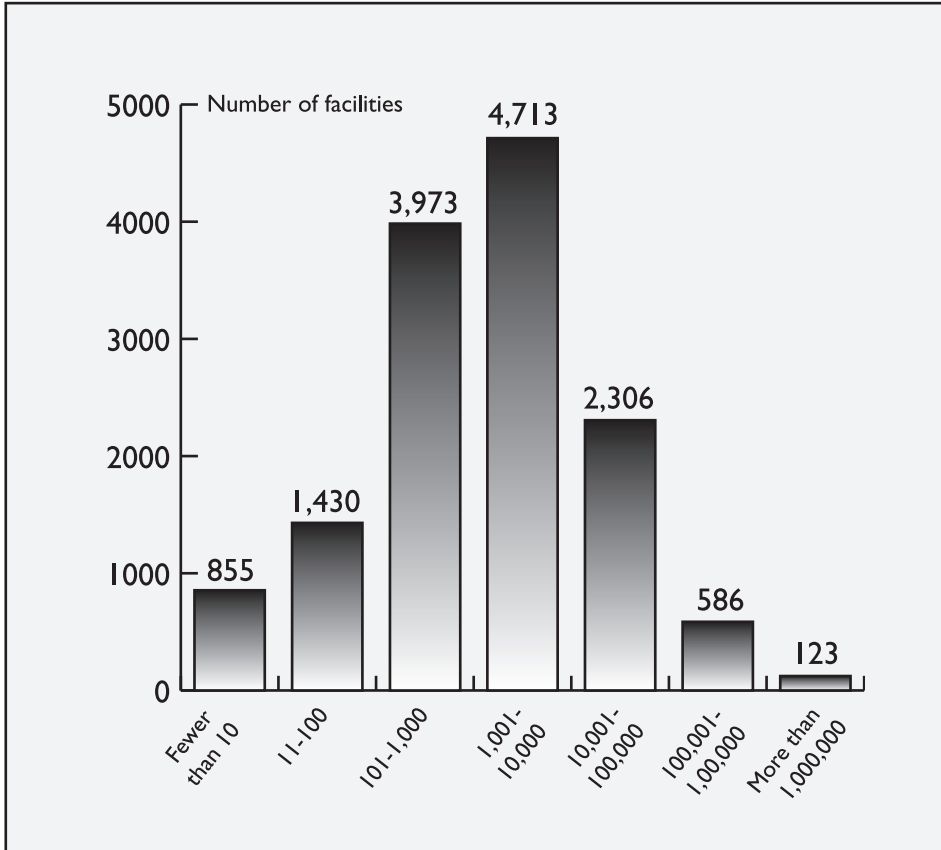
One of the greatest challenges lies in the fact that no one has comprehensively assessed the security of chemical facilities to date. In addition, no federal or state laws explicitly require chemical facilities to assess vulnerabilities or ensure security measures are in place to safeguard their facilities from attack.

Security at chemical facilities is in the hands of the private sector. State officials should be aware of this because improving security at these facilities can be expensive. Unfortunately,

<sup>39</sup>Environmental Protection Agency, Chemical Accidents in U.S. Industry: A Preliminary Analysis of Accidental Risk Data from U.S. Hazardous Chemical Facilities, 25 September, 2000.

<sup>40</sup>Governmental Accounting Office, Homeland Security: Voluntary Initiatives Are Underway at Chemical Facilities, but the Extent of Security Preparedness is Unknown, GAO-03-439, 14 March, 2003, 7.

**Figure 6: Number of Chemical Facilities with “Worst-Case Release” Potential by Residential Population Potentially Threatened**



Source: EPA, Chemical Accidents in U.S. Industry: A Preliminary Analysis of Accidental Risk Data from U.S. Hazardous Chemical Facilities, Washington, D.C.: September 25, 2000.

because the risk profiles of chemical plants differ tremendously due to differences in design, processes, technologies and products, there is no single, specific security regime that would be transferable, appropriate or effective for all chemical facilities. When considering legislation, states must be aware that the chemical sector faces these challenges. Since this sector is vital to our economy, national defense and public health, the goal of any measure or legislation should be to secure without impeding the production of vital chemicals.

### **What are the roles of federal and state government and the private sector?**

Critical infrastructure protection is a complex mission that involves a broad range of functions performed throughout government and the private sector. Protection issues must be dealt with, but because infrastructure protection encompasses such a broad scope, it is foolish to think everything can be fully protected. Therefore national preparedness and response must also be part of our strategy. This combined focus – critical infrastructure protection and incident response – encompasses activities related to national defense, law enforcement, transportation, emergency management, food safety, public health, information technology and other areas. Therefore, for critical infrastructure protection efforts to come even close to being successful, federal, state and local governments and private industry have specific roles and functions that must be integrated.

While the federal government is responsible for broad national security issues, responsi-

---

For critical infrastructure protection efforts to come even close to being successful, federal, state and local governments and private industry have specific roles and functions that must be integrated.

---

---

**The federal government's role is primarily one of coordination and support.**

---

bilities regarding emergency management, local coordination and regulatory issues have historically fallen upon state and local governments. However, given the resources that are necessary to protect the various infrastructure sectors, the range of governmental services that could be affected, and the need for the private sector to be involved in preparing for and mitigating risks, state and local resources alone are insufficient to meet all threats. The unique capabilities, expertise and resources of each critical infrastructure owner/operator are necessary for a comprehensive national protection effort.

Implementing a comprehensive national critical infrastructure effort requires extraordinary organization, clarity of purpose, common understanding of roles and responsibilities, accountability, and a detailed and clear process of coordination. Without these elements, coordinating and integrating a protection strategy, planning, resource management, measuring performance, and acting across federal, state and local governments and the private sector would be impossible.

The overlap of federal, state and local governance and the ownership structure of our critical infrastructures present significant protection challenges. The stakeholders and entities involved, both public and private, are multiple and diverse, and the level of understanding of roles and responsibilities varies. The range of protective activities that each must undertake is vast and changes across infrastructures. And the protection authorities across federal, state and local jurisdictions overlap in many instances and vary greatly.

To this end, it is necessary and helpful to examine the roles of the federal and state governments and the private sector, as outlined in *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, published by the White House in February 2003. This document attempts to clarify these roles in order to achieve the following objectives for critical infrastructure protection:

- Identify and assure the protection of those assets, systems and functions that are deemed most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence.
- Assure the protection of infrastructures that face a specific, imminent threat.
- Pursue collaborative measures and initiatives to assure the protection of potential targets that may become attractive over time.<sup>41</sup>

The federal government essentially launched the infrastructure protection effort with the release of this document because no other publication had gone to such lengths to address the issue of critical infrastructure protection and the roles of the various entities involved. Developed with input from state, local and private entities, the strategy outlines the nation's physical protection goals and clarifies roles and ways in which the federal government will partner with and help the states address infrastructure protection, as well as the efforts expected from states and the private sector.

### **The Federal Role**

The federal government's role is primarily one of coordination and support. Under the Constitution, the federal government has fundamental, clearly defined responsibilities that include providing for the common defense and promoting the general welfare of our people. These responsibilities require the federal government to use military, intelligence and diplomatic assets outside our borders, perform immigration and naturalization functions, conduct vital research, regulate interstate commerce activities, and pursue criminal offenders. Beyond these and other critical services and functions, the federal government has the capacity and responsibility to organize and coordinate across governmental jurisdictions and with the private sector.

In the context of infrastructure protection efforts, the federal role is to coordinate the

<sup>41</sup>The White House, *National Strategy for the Physical Protection of Critical Infrastructure*, 2-3.

efforts and capabilities of state and local governments and private institutions. According to the national strategy, the role involves the following:

- Take stock of our most critical facilities, systems, and functions and monitor their preparedness across sectors and governmental jurisdictions.
- Assure that federal, state, local and private entities work together to protect critical facilities, systems and functions that face an imminent threat and/or whose loss would have significant, national-level consequences.
- Provide and coordinate national threat assessments and warnings that are timely, actionable, and relevant to state, local and private sector partners.
- Create and implement comprehensive, multi-tiered protection policies and programs.
- Explore potential options for enablers and incentives to encourage public and private sector entities to devise solutions to their unique protection impediments.
- Develop protection standards, guidelines and protocols across sectors and jurisdictions.
- Facilitate the exchange of critical infrastructure and key asset protection best practices and vulnerability assessment methodologies.
- Conduct demonstration projects and pilot programs.
- Seed the development and transfer of advanced technologies while taking advantage of private sector expertise and competencies.
- Promote national-level critical infrastructure and key asset protection education and awareness.
- Improve the federal government's ability to work with state and local responders and service providers through partnership.<sup>42</sup>

The strategy also recognizes that each critical infrastructure sector has unique security challenges and it is therefore necessary for the federal government to initiate a plan for each sector. *The National Strategy for Homeland Security*, published in 2002, provided the original sector-based organizational scheme and clarified roles. (See **Figure 7: Federal Organization for Critical Infrastructure Protection**).<sup>43</sup> This organizational scheme identifies the lead federal departments and agencies charged with coordinating protection activities and establishing collaborative relationships with their sector counterparts. In addition to securing federally owned and operated infrastructures and assets, these departments and agencies are to assist state and local governments and private-sector partners in the following efforts:

- Organize and conduct protection and continuity of operations planning, and elevate awareness and understanding of threats and vulnerabilities to critical facilities, systems and functions.
- Identify and promote effective sector-specific, risk-management policies and protection practices and methodologies.
- Expand voluntary, protection-related information sharing among private entities within sectors, as well as between government and private entities.<sup>44</sup>

In addition, the federal government also, in the case of certain sectors, regulates certain activities and imposes federal security requirements on various infrastructures. These include:

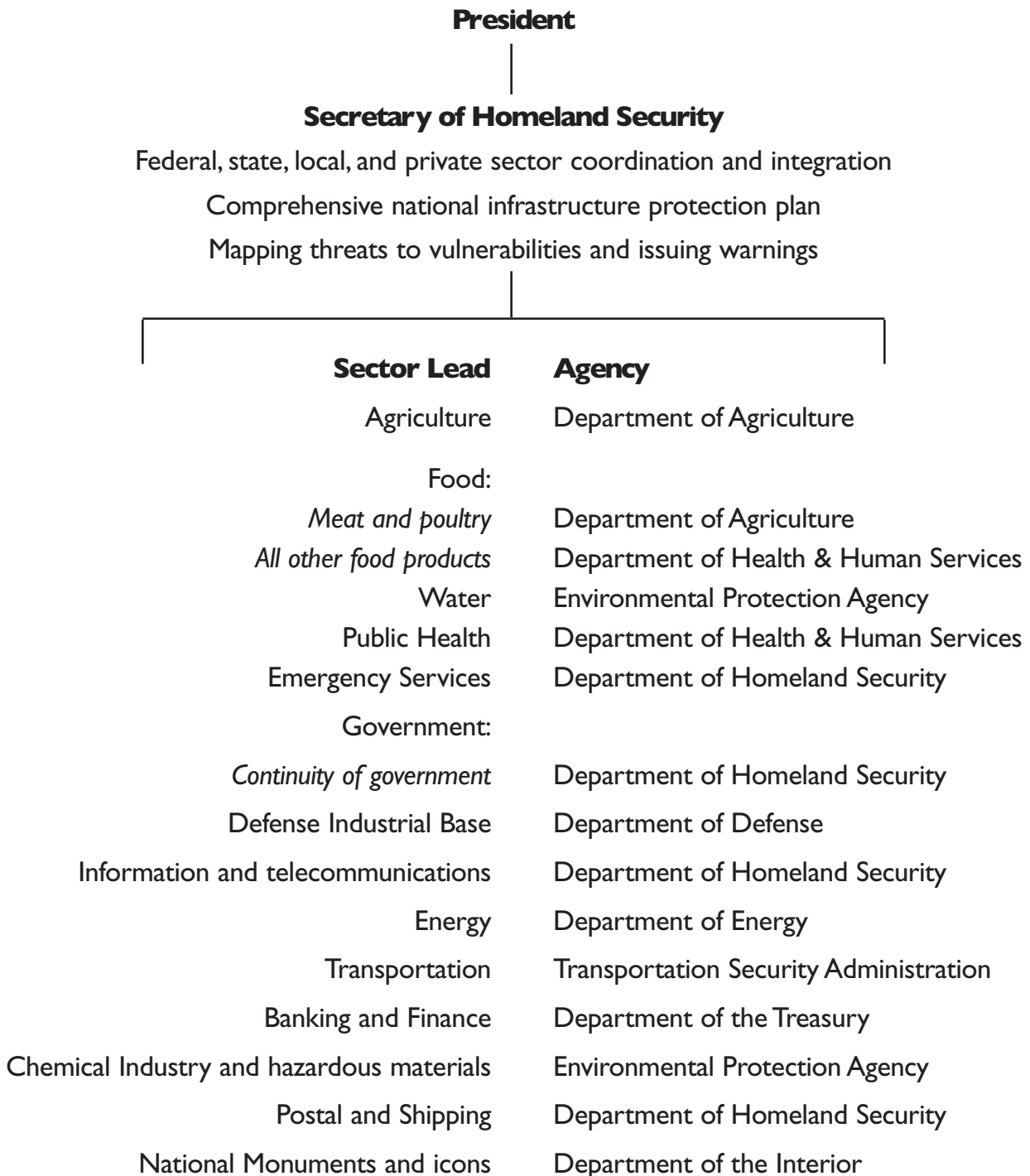
- **Nuclear power plants** – The Nuclear Regulatory Commission subjects all commercial

<sup>42</sup>Taken from the Critical Infrastructure Strategy document.

<sup>43</sup>The White House, *The National Strategy for Homeland Security*, July 2002.

<sup>44</sup>The White House, *National Strategy for the Physical Protection of Critical Infrastructure*, 17.

## Figure 7: Federal Government Organization for Protection of Critical Infrastructure and Key Assets



plants to security requirements, including physical barriers outside the operating areas, limited access restrictions, trained security forces and simulated attack exercises.

- **Community water systems** – The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires community water systems that serve more than 3,300 people to conduct vulnerability assessments, prepare emergency response plans, certify them to the EPA and provide EPA with a copy.
- **Maritime** – The Maritime Transportation Security Act of 2002 requires the Department of Homeland Security to identify ports and vessels that pose high security risks and to conduct assessments of these ports and vessels.
- **Aviation** – The Aviation and Transportation Security Act of 2001 transferred aviation security from the Federal Aviation Administration to the Transportation Security Administration and directed the agency to undertake airport screening activities.

### The State Role

The critical infrastructure protection mission at the state and local level involves 50 states, four territories, the Commonwealth of Puerto Rico and 87,000 local jurisdictions. Many have already gotten off to a good start as all states and territories have established homeland security offices to manage their infrastructure protection efforts, along with other security issues. And, of course, the states have law enforcement agencies, National Guard units and other critical services that can and should be employed in this mission when necessary.

The national strategy for physical protection lays out areas of concern for states and activities in which states can engage to help achieve our country's infrastructure protection objectives. States are tasked, with the support of federal lead departments and agencies, with the following:

- Promote the coordination of protective and emergency response activities and resource support among local jurisdictions and among regional partners.
- Determine criticality of infrastructure, prioritize investments in protection efforts and hold preparedness exercises within the state and regionally in conjunction with other states.
- Help local jurisdictions and the private sector obtain federal assistance when the required levels of preparedness exceed their resources.
- Facilitate the exchange of relevant security information and threat alerts down to the local level.<sup>45</sup>

While attempting to assign states these roles in protecting infrastructure, the federal government hopes to provide a single point of coordination for state and local governments for infrastructure protection issues through the Department of Homeland Security. Certainly state and local governments will look to the federal government for support and resources when requirements exceed their capabilities. With regard to specific sector issues, the national strategy directs the lead federal departments and agencies and federal law enforcement organizations to provide support as needed.

Regardless of whether this help is provided or not, states must recognize that they are on the front lines. Regardless of who owns and operates the affected infrastructure during an incident or attack, state and local authorities and communities must respond immediately. Many states have well-organized relationships with one another through various organizations, partnerships, and mutual support agreements, which they should take advantage of when federal resources are scarce. Coordinating with one another allows states to capitalize on their mutual capabilities through regional approaches. Examples of such successful efforts will be discussed in the next chapter.

---

**The critical infrastructure protection mission at the state and local level involves 50 states, four territories, the Commonwealth of Puerto Rico and 87,000 local jurisdictions.**

---

<sup>45</sup>ibid, 19-20.

**The unique characteristics of critical infrastructures, their evolving nature, and the challenges complicating their protection will require an unprecedented level of public/private cooperation and coordination.**

### **The Private Sector Role**

Approximately 85 percent of our critical infrastructures are owned and operated by the private sector. While these industries have always been responsible for protecting their physical assets, the threat of terrorism, with its potential severe economic and psychological impacts, is relatively new for many of them. Still, the private sector remains the first line of defense. The national strategy recognizes that most private companies determine their levels of investment in security based on the following:

- what is known about the risk environment or threat
- what is economically justifiable
- what is sustainable in a competitive marketplace or on limited resources

The national strategy also outlines ways the private sector can improve on its security posture and help improve its protection responsibilities, including the following:

- Reassess and adjust planning, assurance and investment programs to accommodate increased risks.
- Make prudent investments earlier and at all levels of the risk management spectrum.
- Seek to develop mutually beneficial relationships and coordination protection efforts with the public sector.
- Seek or continue to develop sector alliances in order to sustain reliability and share operational and security-related best practices.
- Work within sectors to develop mutual aid agreements to prevent disruption of one member's systems from cascading across the sector.

The national strategy also recognizes that, given the nature of threats today and the severity of the potential consequences, the private sector will look to government to help inform its decisions on security investments and will require assistance when the threat exceeds the operator's capability to protect itself beyond a reasonable level. To this end, the federal government has pledged to collaborate with states and other public and private sector entities to protect infrastructures.

In the end, protecting critical infrastructures will require a close and well-organized partnership among all levels of government and the private sector. The unique characteristics of critical infrastructures, their evolving nature, and the challenges complicating their protection will require an unprecedented level of public/private cooperation and coordination.

### **What are the legal aspects of critical infrastructure protection?**

A range of legal and administrative activity has emerged regarding critical infrastructure protection since September 11 under the auspices of homeland security. The legal framework of critical infrastructure protection is a moving target that continues to change. The scope of legal issues and the range of perspectives on issues associated with critical infrastructure protection are vast.

Understanding the many complexities involved in making law to protect critical infrastructure begins with the observation that threats to infrastructure, the means and activities necessary to secure it, and even the state of infrastructures themselves all continually evolve.

The legal landscape, therefore, is also continually changing. It is beyond the scope of this guide to cover all the legal aspects regarding critical infrastructure protection. Indeed, as many of these legal issues are currently amorphous and still evolving, any broad examination may be outdated within a period of months. However, we will attempt to deal with those legal issues currently of most concern for states.

The law as it applies to critical infrastructure protection involves statutes enacted by Congress and state legislatures, and regulations promulgated by federal and state government agencies, many of which were put in place to address specific issues characteristic of each regulated area. Therefore, many parties have jurisdiction to make law concerning some part of the nation's critical infrastructure. The legal issues that states are currently dealing with when making critical infrastructure policy stem almost completely from issues regarding information sharing, including questions regarding information protection, privacy, right-to-know issues, anti-trust issues, and even liability issues.

## Information Sharing

Perhaps the most important policy issues regarding critical infrastructure protection, both at the federal and state levels, relate to information sharing: who shares information, who it is shared with, and under what circumstances. Collectively, these policies are governed by federal and state statutes known as freedom of information act (FOIA) policies or freedom of information laws (FOIL). While several states have come up with various legislation regarding infrastructure, which will be discussed in the next chapter, states have really only been able to comprehensively address critical infrastructure protection legislatively through the use of freedom of information laws.

The purpose of the federal Freedom of Information Act (FOIA) was to ensure, by statute, citizen access to government information. The FOIA establishes for any person – corporate or individual, regardless of nationality – access to existing, unpublished agency records on any topic. The law specifies nine categories of information that may be exempted from the rule of disclosure. The exemptions permit, rather than require, the withholding of requested information. Records which are not exempt must be made available. If a record has some exempt material, any portion of the record that may be reasonably segregated from the entire record must be provided to any person who requests it after the exempt portions are deleted. Disputes over the accessibility of requested records may be reviewed in federal court. Three of the act's nine exemptions from public disclosure provide possible protections against the release of homeland security and critical infrastructure information. These include Exemption 1 (national security information), Exemption 3 (information exempted by statute), and Exemption 4 (confidential business information).<sup>46</sup>

The federal government's Homeland Security Act created new exemptions to the federal and state Freedom of Information laws. The Critical Infrastructure Information Act, part of the Homeland Security Law, states that when a business voluntarily submits "critical infrastructure information" to the Department of Homeland Security, it is exempt from the federal FOIA. Further, if the federal government gives that information to a state, then that information is exempt from the state FOIL as well. The law also grants businesses immunity from civil liability for violations of securities law; civil rights laws; environmental, labor and consumer protections; and health and safety laws, should such violations be revealed in the information they provide the department.

Proponents have called for restricting access to certain types of information, both at the state and federal levels, because they worry that it could contain details on critical systems that people intent on doing harm could use to discern vulnerabilities. However, many critics feel that exemptions to freedom of information laws are unconstitutional. The public, they say, needs access to information about threats confronting the nation. The question facing policy-makers is how to balance the public's right to know about threats and the costs involved in meeting those threats with the possibility that the information itself will increase the threat and expose us to greater risks.

On the other end of the spectrum, the private sector has various concerns about the

<sup>46</sup>See 5 U.S.C. § 552(b).

benefits, necessity and liabilities of sharing information with the public sector and with other companies. For example, many in the private sector believe that information sharing could lead to allegations of price fixing, restraint of trade, charges of discrimination against customers, trade secrets being revealed and the exposure of vulnerabilities or weaknesses that could erode public confidence in their business or operations.

## Chapter Three



**What are the states currently doing and what future action is necessary?**

## What are states doing to protect critical infrastructure?

America's critical infrastructures provide the foundation for our way of life and are crucial to national security, economic vitality and public health. Although we have long relied on these sectors, the concept of critical infrastructure protection is fairly new. Born out of the concept of homeland security and the realization of our vulnerabilities that pervaded the post-September 11 environment, the issue of protecting our critical infrastructures and assets is here to stay. The need to secure our critical infrastructure is apparent – not just from future terrorist attacks, but from all major disasters and events that could disrupt and threaten our way of life.

To begin to address the many policy issues that arise when considering critical infrastructure protection, it will be helpful for state officials to know what other states are currently doing in this area. Unfortunately, states' responses to critical infrastructure issues have been somewhat limited due to the following issues:

- infrastructure protection as a new concept
- information sharing problems
- focus on response more so than protection
- budget problems

In many ways, states effectively started from scratch after September 11 in dealing with these issues. Now many states have homeland security offices and directors focused on coordination, planning and response, legislative committees to provide oversight, and they have begun efforts to interface with federal and local governments and the private sector. But such actions and responses are broad in scope and very complex and take years to develop effectively.

Information sharing has also been an issue at the state level. Communication between the federal and state governments and between states and the private sector has been difficult, due to the sensitivity of information related to infrastructure threats. Many of the legal issues surrounding information sharing were described in Chapter 2. More than two years after September 11, states are still tackling these challenges.

In addition, as a result of the emphasis on preparing for future terrorist attacks that followed September 11, the focus on a buildup of readiness capabilities has detracted somewhat from infrastructure protection. Although many states have worked to secure critical facilities, important government buildings and other assets, overall, states have focused more on responding to attacks and protecting public health after attacks than on protecting infrastructure from attacks. They have spent billions of dollars equipping emergency first responders, public health facilities and hospitals, and law enforcement with the training and equipment necessary to respond to terrorist attacks. The resources allocated to response efforts will no doubt have a huge effect on improving responses to terrorist attacks and to other events. And, given states' current fiscal problems, the resources to address many protection needs are simply not there.

States are attempting to do more, but due to the limitations discussed above they have really only been able to address critical infrastructure protection through two ways: legislation and partnerships.

## State Legislation

While some states have passed various laws, many have only really been able to address critical infrastructure protection, as discussed earlier, through freedom of information laws. State budget problems have limited what protection measures they can feasibly enact. Also, since critical infrastructure protection is still a new concept, many states are still conducting assessments and studies of the feasibility of various protection measures and the vulnerabili-

ties that exist within their borders. In addition, some people see many potential security and protection measures as fairly restrictive and costly to the private sector. Many states have been wary of imposing legislation that could weaken their economies by driving out businesses or curbing their output.

Despite these limitations, states have responded to the concept of critical infrastructure protection under the mantle of homeland defense. After September 11, many states established homeland security departments or offices, appointed a director of homeland security, and gave these entities authority to oversee protection of infrastructure. Alabama, for example, enacted HB 335, the Alabama Homeland Security Act of 2003, which created the state's Department of Homeland Security with the following powers and duties:

- Coordinate the states' efforts to protect its critical infrastructures, including, but not limited to, energy production, transmission and distribution systems, telecommunications, nuclear facilities, public and privately owned information systems, transportation hubs and networks, livestock, water and food supplies.
- Ensure that state, county and local governmental agencies and authorities coordinate and cooperate with the private sector infrastructure owners and operators for the protection of critical infrastructure.
- Impose security requirements in a manner consistent with federal law and regulations, including measures adopted by federal agencies responsible for infrastructure protection, such as the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, and the Department of Homeland Security.

In addition to legislation creating departments to oversee infrastructure and homeland security, states have passed legislation authorizing the use of state resources to conduct vulnerability assessments on various infrastructure areas so the state can decide what to secure and how best to secure it. Some measures also give the governor and other state agencies the authority to require certain utilities and private sector infrastructure owners/operators to perform such assessments using their own resources, allowing these sectors to use their own expertise to evaluate their vulnerabilities. In other cases, state advisory bodies are created to help guide the infrastructure protection efforts and studies. Examples of states that have enacted such measures include the following:

- Iowa – HF 762 authorizes the governor and other state agencies to conduct studies and surveys of any industries, resources or facilities within the state as necessary to ascertain the vulnerabilities of critical state infrastructure and assets. It also established a separate Task Force on Homeland Security and Defense to study and report on the state's preparedness to respond to threats and examine issues related to the detection, prevention, preemption and deterrence of attacks aimed at, among other things, state infrastructure.
- Nevada – AB 441 requires certain utilities to conduct vulnerability assessments and prepare emergency response plans. In addition, it also created the Nevada Commission on Homeland Security, which among its duties is responsible for studying and identifying infrastructure "according to their susceptibility and need for protection."
- Virginia – HB 2210 authorizes the governor and other states agencies to conduct studies of critical infrastructure to prevent or reduce the harmful consequences of attacks and disasters.
- Texas – HB 9 requires the governor to develop and direct a statewide security strategy. It also created a state critical infrastructure protection council to advise the governor on developing the elements of the strategy pertaining to critical infrastructure.

While states have enacted various measures such as those described above, they are somewhat broad in scope. They apply mostly to coordination of efforts and study of vulnerabilities, but they do not necessarily outline specific steps. Again, this is attributable to the vari-

ous reasons mentioned before: the possible detrimental effects on state economies, state budget problems, and the newness of infrastructure protection as a concept, which requires states to take a slow approach. At the urging of the federal government, however, many states have taken steps to pass legislation with specific guidelines regarding information sharing and the disclosure of information regarding critical infrastructure.

### **What actions have states taken regarding information sharing?**

Before September 11, some states already had comprehensive information-disclosure statutes in place that addressed terrorism concerns and critical infrastructure. Florida, Michigan, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Oregon, Utah, Virginia and Washington all had comprehensive statutes.

Since September 11, states have looked carefully at their FOIA policies and many have attempted to balance the public's right to know with concerns about security. Numerous states have exempted security-related information from state FOIA requirements, have exempted information under certain circumstances, or have given state agencies the authority to exempt themselves from FOIA requirements.

Many states, therefore, now have exemptions that address some of the federal concerns about information disclosure. Since September 11, 32 states have altered their FOIA laws or have passed new confidentiality laws to protect security-related information, which by definition includes critical infrastructure information:

Alaska	Michigan
Arizona	Missouri
Arkansas	Nevada
California	New Hampshire
Colorado	New Jersey
Connecticut	New Mexico
Delaware	North Dakota
Florida	Ohio
Georgia	Oklahoma
Idaho	Rhode Island
Illinois	Texas
Kansas	Utah
Louisiana	Virginia
Maine	West Virginia
Maryland	Wyoming
Massachusetts	Washington

States have taken action to secure information regarding critical infrastructure; however the test of these new laws will surely come in the courts and from attempts to designate what information fits into the categories defined in the laws.

### **Partnerships**

The other main tool states have used to strengthen critical infrastructure protection is partnerships with other states and entities. Many infrastructures extend well beyond state boundaries, including power transmission lines, pipelines, telecommunications lines, major highways and rail lines. Some infrastructures even cross national frontiers. Eighty percent of

the natural gas consumed on the West Coast, for example, comes from Western Canada. Regional partnerships, both public and private, allow states and other stakeholders to more successfully accomplish many facets of the infrastructure protection mission. Partnerships allow stakeholders to share resources, improve communication and coordination, and formulate exercises and scenarios to respond to, which help them quickly identify vulnerabilities. Further, partnerships help the states overcome many of the legal, organizational and cultural barriers that prevent effective communication and teamwork. This section will highlight some current partnerships between states, and also between states and other public and private entities, that are resulting in innovative and useful mechanisms for protecting critical infrastructure.

### **Partnership for Regional Infrastructure Security**

One well-known infrastructure security partnership was formed after September 11 by the Pacific North West Economic Region (PNWER). In the summer of 2002, PNWER held the second in a series of exercises as part of an ongoing initiative known as the **Partnership for Regional Infrastructure Security**. PNWER is a public/private partnership that has existed since 1991 to facilitate cooperation, coordination and communication among its members. Its goal is to enhance the economic development of its eight U.S. and Canadian member jurisdictions: Alaska, Idaho, Oregon, Montana, Washington, Alberta, British Columbia and the Yukon Territory.

To develop a better understanding of the region's critical infrastructure and associated interdependencies, the Partnership for Regional Infrastructure Security was launched in late 2001 with an initial meeting of more than 120 public and private sector organizations from all the PNWER jurisdictions. The partnership's goal is to develop a cooperative preparedness strategy that will enhance the security of critical infrastructure systems throughout the region. The table-top exercise conducted last summer, titled "Blue Cascades," brought together more than 150 representatives from 70 public and private sector organizations for a cross-border, multijurisdictional exercise to examine infrastructure interdependencies. The exercise involved PNWER, the Federal Emergency Management Agency, the U.S. Navy, and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness.

Developed by PNWER members representing the public and private sectors, the scenario focused on attacks that had the ability to cause cascading, long-term impacts. Therefore, the scenario began with disruptions to physical infrastructure that quickly spread to other critical areas. PNWER's exercises focused on high-voltage transmission grids, natural gas and oil pipelines, and the telecommunications industry.

Each participant reacted to different disaster scenarios. The simulated attacks caused region-wide power outages that spread to other Western states and were followed by disruptions of the region's natural gas distribution, telecommunications systems and simulated threats to the water supply systems. Other infrastructure and critical services throughout the region were affected by the disruptions, including transportation, law enforcement and emergency services.

The partnership has helped highlight the challenges and cross-border issues that could arise from such disruptions and has helped public and private sector participants identify the many challenges that result from infrastructure interdependencies. By cooperating, public and private sector representatives quickly identified interconnected weaknesses and vulnerabilities.

### **New Jersey Business Force**

The New Jersey Business Force, a first-of-its-kind partnership between New Jersey and leading companies in the state, is an innovative solution to America's continuing vulnerability to attacks on the homeland. The project is being built by Business Executives for National

Security (BENS), a nationwide, nonpartisan organization that serves as a channel through which senior business executives help enhance the nation's security. As of March 2003, charter members included The Amelior Foundation, Atlantic Health System, Automatic Data Processing Inc., The CIT Group Inc., DRS Technologies, KPMG LLP, Pfizer Inc., Prudential Financial, Saint Barnabas Health Care System, Stevens Institute of Technology, United Retail Group Inc., and Verizon Communications.

The New Jersey Business Force will focus on high priority areas where the unique expertise of the private sector can complement ongoing state efforts and provide genuine contributions in preparing for and responding to catastrophic events or terrorists attacks. For example:

- An Internet-based Business Response Network will inventory the capabilities needed in an emergency – transportation, warehouses, communications, medical supplies, construction equipment – and identify companies willing to provide these services on short notice.
- A Business Volunteer Training Program will prepare companies and employee volunteers to perform discrete tasks that the state requires but lacks resources to execute in an emergency or to rehearse in advance.
- A Rapid Medical Distribution Plan will draw on resources of participating transportation, trucking, shipping and freight companies to ensure that vital medical supplies reach hospitals during an outbreak of an infectious disease.

BENS plans to promote the New Jersey Business Force as a model for other states, providing businesses and their employees with a way to help protect their communities and our economic security. This partnership is a good example of how private stakeholders can participate in a way that is effective, improves coordination and communication, and makes critical infrastructure more secure.<sup>47</sup>

### **New York State Office of Cyber Security and Critical Infrastructure Coordination**

The New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) is responsible for leading and coordinating the state's efforts regarding cyber security, geographic information systems (GIS) and critical infrastructure preparedness. CSCIC works collaboratively with the public and private sectors to foster communication and coordination. While the office is not in itself a partnership initiative, it has given birth to three infrastructure partnerships:

- The Public/Private Sector Cyber Security Workgroup
- The New York Cyber Security and Infrastructure Protection Initiative
- The Multi-State Information Sharing and Analysis Center (Multi-State ISAC)

The Public/Private Sector Cyber Security Workgroup facilitates information sharing between the public and private sectors. Comprised of representatives of private-sector industries and government agencies, the workgroup meets regularly to exchange information about threats and risks to the state's critical infrastructures. That information is then funneled back to the CSCIC. The workgroup identified 13 critical sectors and chose eight upon which to initially focus its cyber security efforts: Financial and Economic, Health, Telecommunications, Utilities, Government, Transportation, Education and Awareness, and Public Safety. While the group's work is ongoing, it has made recommendations to New York's public and private sectors regarding vulnerabilities, risk assessments, developing emergency response capabilities, and developing both legal and technical advisory bodies.

<sup>47</sup>The Council of State Governments, "Infrastructure Security in the States: Bridging the public and private gap," Homeland Security Brief, April 2003, 3.

The New York Cyber Security and Infrastructure Protection Initiative was launched in 2002 to promote partnerships and private sector involvement within the state. The initiative has identified 13 major sectors in which critical infrastructures need protection and has assigned public and private sector representatives to collaborate on plans and efforts to protect sector-specific infrastructures.

The Multi-State Information Sharing and Analysis Center (ISAC) will be covered in the following section. This effort and the ones described above demonstrate that New York is doing model work in the area of critical infrastructure protection and partnerships.

### **Multi-State Information Sharing Analysis Center**

Formed and currently coordinated by the New York State Office of Cyber Security and Critical Infrastructure, the Multi-State Information Sharing and Analysis Center facilitates communication among states regarding cyber and/or critical infrastructure readiness and response efforts. It is currently being used as a clearinghouse to exchange information about the status of other states' critical infrastructures, both cyber and physical.

Launched in January 2003, the Multi-State ISAC has already grown to include 20 member states that meet monthly by teleconference to discuss operation and readiness issues. Forty-six states (including the 20 members) receive and send critical infrastructure information via the ISAC. Serving as a central repository for information about cyber-security breaches and infrastructure threats, the center gathers data from public- and private-sector members. States participating in the Multi-State ISAC are listed below, with member states in bold:

<b>Alabama</b>	Missouri
<b>Alaska</b>	<b>Montana</b>
<b>Arizona</b>	Nebraska
Arkansas	<b>Nevada</b>
California	New Hampshire
<b>Colorado</b>	New Jersey
Connecticut	<b>New Mexico</b>
Delaware	<b>New York</b>
<b>Florida</b>	North Dakota
Georgia	Ohio
Hawaii	Oklahoma
<b>Idaho</b>	<b>Oregon</b>
Illinois	<b>Pennsylvania</b>
<b>Indiana</b>	<b>Rhode Island</b>
Iowa	South Carolina
<b>Kentucky</b>	South Dakota
<b>Louisiana</b>	Tennessee
Maine	Texas
Maryland	Utah
Massachusetts	<b>Vermont</b>
Michigan	<b>Washington</b>
<b>Minnesota</b>	Wisconsin
Mississippi	<b>Wyoming</b>

The center's goals are to increase real-time sharing of information, eliminate states' needs to build or develop redundant applications or tools, and strengthen infrastructure protection. This partnership's rapid success makes it a model for sharing information among state governments about critical infrastructure readiness and vulnerabilities.

### **Principles for a Comprehensive Security Strategy: An Evaluation Guide for the Transportation Industry**

Another interesting partnership initiative has led to a Transportation Security Evaluation Guide for states. A federal/state partnership that included five states and the Domestic Working Group of the General Accounting Office created the guide to assist auditors and transportation personnel in assessing the security programs for states' transportation assets and operations. Louisiana, Arkansas, Connecticut, New York and Rhode Island participated in the project, with Louisiana as the lead state.

The final report, prepared by Louisiana's Legislative Auditor, describes the principles for developing and maintaining an effective, economical and comprehensive transportation security strategy. The guide is divided into three main sections:

- **Principles for conducting risk assessments** – The guide provides state officials with a step-by-step description of the risk assessment process and a basic framework for identifying critical transportation infrastructure and possible threats and for assessing vulnerabilities.
- **Principles for developing and maintaining countermeasures** – The guide includes a methodology for developing and maintaining effective and economical security strategies.
- **Principles for emergency preparedness** – It also describes the key elements required for emergency preparedness.<sup>48</sup>

The guide provides checklists for each set of principles to aid in assessment. Since the document is not specific to any one mode of transportation, it can be adapted and modified to fit a state's specific needs. The aim of the guide is to serve as a standard for states and security auditors to effectively evaluate transportation security and aid in management of transportation security programs. Since such an approach could be transferable to other infrastructure sectors, this initiative shows that states and the federal government can collaborate to produce innovative tools to help states secure critical infrastructure.

### **New Mexico Critical Infrastructure Assurance Council**

One final effort worth mentioning is The New Mexico Critical Infrastructure Assurance Council (NMCIAC). While the council has struggled since it was developed in 1998, it is worth highlighting here because it is perhaps the only pre-September 11 critical infrastructure protection partnership. Efforts to revive it are underway by the New Mexico Institute for Mining and Technology, which has taken over the project from the University of New Mexico.

NMCIAC is a cooperative, public/private partnership to exchange information among the private sector, educational institutions, state government, the Federal Bureau of Investigation, and other federal and local agencies in order to ensure the protection of critical infrastructure in New Mexico. By sharing and disseminating information about threats to critical systems, the council attempted to promote the protection of physical and cyber assets. NMCIAC sought to become a conduit through which to addresses threats, vulnerabilities, countermeasures and responses to infrastructure attacks, and other actions that may affect member organizations or the public. However, the council has not been able to entirely accomplish this for various reasons.

<sup>48</sup>State of Louisiana Legislative Auditor; Principles For A Comprehensive Security Strategy: An Evaluation Guide for the Transportation Industry, October 2002. <<http://www.la.state.la.us/perform/tseg02.pdf>> (23 July 2003).

---

**With the multitude of stakeholders across the many different infrastructures and the layers of responsible parties, successful coordination and communication efforts will continue to be paramount.**

---



---

**Two of the biggest challenges facing states are identifying and verifying critical infrastructures, and developing or modifying plans to secure them.**

---

In response to ideas that emerged from the President's Commission on Critical Infrastructure Protection (described in Chapter 1), the University of New Mexico partnered with the FBI and the New Mexico Department of Public Safety to sponsor meetings in 1998 to discuss responses. NMCIAC was developed and identified as a method to meet the state's needs for critical infrastructure protection and as a model that other states could adopt to do the following:

- Establish rapid communication of threats and attacks.
- Encourage private/public collaboration.
- Identify critical infrastructures.
- Determine local response methods and the role of first responders.<sup>49</sup>

While the project got off to an ambitious start, it suffered from a lack of sustained funding, lack of interest by the private sector, and lack of cooperation by the various state agencies, which continued to focus on their own respective areas. However, efforts are underway to revive the project. Despite the council's shortcomings, other states could benefit from NMCIAC's example as the first pre-September 11 state partnership for protecting critical infrastructure.

### **What can states do in the future?**

As we have highlighted, states are doing many things to address critical infrastructure protection, but state activity has been somewhat limited and there is room for additional action. Given the role of critical infrastructure in ensuring the United States' economic and national security, public health and overall well-being, the importance of protecting these systems from attack or disruption cannot be disputed.

This section will highlight some themes that have emerged from this guide that states should focus on to improve protection of their critical infrastructure assets. This includes taking steps to do the following:

- Focus on coordination, communication and information sharing efforts.
- Focus on partnerships with other states, the federal government and the private sector.
- Conduct scenario-based exercises.
- Work on risk assessments and identifying critical assets and vulnerabilities.

With the multitude of stakeholders across the many different infrastructures and the layers of responsible parties, successful coordination and communication efforts will continue to be paramount. Successful information-sharing efforts, like the Multi-State Information Sharing and Analysis Center, can help facilitate this process and allow states to prevent duplication of efforts, share resources, and help ensure successful coordination of efforts across multiple jurisdictions.

Other forms of partnerships can have similar effects, allowing states and other private and public stakeholders to communicate more effectively and coordinate protection and response efforts. Through partnerships, stakeholders can share resources, prevent duplication of efforts and technologies, and discuss and practice responses so that all parties are prepared.

Two of the biggest challenges facing states are identifying and verifying critical infrastructures, and developing or modifying plans to secure them. These tasks cannot be completed in a vacuum and require the involvement of many stakeholders, including the private sector, law enforcement, first responders, the military, and state, local and federal government entities. Effective partnerships can facilitate this collaboration by tapping pre-established relationships that develop from partnering activities.

<sup>49</sup> Daniel J. O'Neil, "Statewide Critical Infrastructure Protection: New Mexico's Model," TR News, vol. 211 (November-December 2000): 25-26.

States should also proactively conduct exercises related to critical infrastructure protection. By conducting response and readiness exercises, states can quickly identify vulnerabilities and areas that need added attention, thereby allowing them and other stakeholders to develop or modify security plans more quickly and effectively.

The first step in developing and implementing a robust infrastructure protection strategy is identifying critical assets. States must conduct thorough and comprehensive assessments of facilities and infrastructure networks to identify vulnerabilities, and they must make sure these assessments are always up to date. However, due to limited resources, governments and private companies cannot adequately protect every asset, and officials must undertake some risk assessment and risk management to identify the most vital critical infrastructures in their states.

State officials need to ask themselves questions such as: Is a nuclear power plant a critical infrastructure for our state or for neighboring states or both? Is a bridge connecting two states across a river a critical infrastructure? Is a certain chemical facility a critical asset and does not protecting it pose a danger to the surrounding population? What infrastructure may require uniform protective measures? Which neighboring states need to be prepared for potential disasters at which infrastructures? Officials should also realize that critical infrastructures for a city may not be critical for the entire state.

Many private industries are caught in these often confusing questions and struggle to determine what is critical and what measures must be implemented. Additionally, some critical infrastructures are owned and operated by the private or public sectors while others are owned and operated by quasi-public/private entities. A few may even be owned or operated and highly regulated by the federal government, making it difficult for state and local officials to develop plans for additional protection and response measures.

To face these difficult challenges, states need to implement measures to focus on and ensure successful communication, coordination and information sharing. They should form partnerships, conduct exercises to more quickly and successfully identify needs, and they should use risk management practices to help protect the most important critical infrastructures.

## Conclusion

This guide has highlighted the diverse characteristics of our different critical infrastructures and the physical protection challenges that states face. It has presented information on what states are currently doing to address this issue and future actions they can take. However, this is merely an introduction to an issue that states will be dealing with for some time to come.

As states work to address the many infrastructure protection challenges, it is important to remember the complex nature of the infrastructures and assets that are to be protected. As potential targets for terrorists, the United States' critical infrastructures are a highly diverse, interdependent mix of facilities and networks. As we have discussed, governments own and operate some of them, but most are controlled by the private sector. However, all are vulnerable in some way to the terrorist threat. Failure in one infrastructure can cascade to cause disruption or failure in others, and the consequences for states and the public can be massive. States must understand these complexities as they work to implement future strategies and plans to protect critical infrastructure.

September 11 proved that all disasters and disruptions, no matter the scope, are local events in that they require response and management at the state and local levels. State and local governments play vital roles not only in responding to disasters, but also in protecting critical infrastructures from attack. Therefore, states must work to understand the challenges, to be prepared, and to be active partners with all critical infrastructure counterparts and stakeholders for the sake of public safety and our economic and national security.





## **Appendices**

- **Critical Infrastructure**  
**Acronyms**
- **Glossary of Terms**



**Appendix A:****CRITICAL INFRASTRUCTURE ACRONYMS**

The following is a list of acronyms that may be encountered when dealing with critical infrastructure protection issues. While some were used in this publication, others were not but could be encountered in various situations involving infrastructure protection.

**A**

A & I	assurance and integration
ABA	American Bankers Association
ACC	American Chemistry Council
AFB	Air Force base
AICPA	American Institute of Certified Public Accountants
AMWA	Association of Metropolitan Water Agencies
APHIS	Animal and Plant Health Inspection Service
API	American Petroleum Institute
ASCE	American Society of Civil Engineers
ASIMS	automated security intrusion monitoring system
ASTM	American Society for Testing and Materials
ATF	Bureau of Alcohol, Tobacco and Firearms
ATM	automatic teller machine

**B**

BW	biological warfare
----	--------------------

**C**

C3	command, control and communications
C3I	command, control, communications and intelligence
C3I/SR	command, control, communication/surveillance and reconnaissance
CA	certificate authority
CBI	confidential business information
CBIRF	Chemical, Biological Incident Response Force
CBO	Congressional Budget Office
CBR	chemical, biological or radiological
CCR	Central Contractor Registry
CDC	Centers for Disease Control and Prevention
CDMA	code division multiple access
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordination Group
CID	Criminal Investigation Division
CINC	Commander-in-Chief
CIO	Chief Information Officer
CIP	critical infrastructure protection
CIP IWG	Critical Infrastructure Protection Interagency Working Group
CIRT	Computer Incident Response Team
CISSP	certification for the information systems security profession
CIWG	Critical Infrastructure Working Group
CMRS	commercial mobile radio service
CNA	computer network attack
CNE	computer network exploitation

COG	continuity of government
COM	component object model
COMSEC	communications security
CONUS	Continental United States
COOP	continuity of operations plan
COTS	commercial off-the-shelf
CPAS	cellular priority access service
CRS	Congressional Research Service
CSIRC	computer security incidence response capability
CSIRT	Computer Security Incident Response Team
CST	Central Standard Time
CSTB	Computer Science and Telecommunications Board
CTRT	Counter-Terrorism Response Team
CW	chemical weapons
CWA	Clean Water Act

## D

DARPA	Defense Advanced Research Projects Agency
DCE	distributed computing environment
DCI	Director of Central Intelligence
DDOS	distributed denial-of-service attack
DEA	Drug Enforcement Agency
DEST	Domestic Emergency Response Team
DFO	disaster field office
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIAP	Defense-Wide Information Assurance Program
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLA	Defense Logistics Agency
DMS	defense message system
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DoI	Department of the Interior
DoJ	Department of Justice
DoL	Department of Labor
DoS	Department of State
DoT	Department of Transportation
DSL	digital subscriber line
DSS	Defense Security Service
DTRA	DoD Threat Reduction Agency
DUNS	Dunn & Bradstreet identification code
DVA	Department of Veterans Affairs

## E

EAL	encryption agreement license
EC	electronic commerce
ECPA	Electronic Communications Privacy Act
EDAMS	electronic document & management systems
EDI	electronic data interchange
EHV	extra high voltage

EIA	Energy Information Administration
EKMS	electronic key management system
EMP	electromagnetic pulse
EMS	emergency medical service
EO	Executive Order
EOC	emergency operations center
EOP	Executive Office of the President
EPA	Environmental Protection Agency
ERAMS	environmental radiation ambient monitoring system
ERP	enterprise resource planning
ERT	emergency response team
EST	Eastern Standard Time

## F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FDIC	Federal Deposit Insurance Corporation
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FIDNet	Federal Intrusion Detection Network
FIFO	first-in-first-out
FIM	federation interface manager
FIPS	federal information processing standard
FLE	federal law enforcement
FOC	full operating capability
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
FRP	Federal Response Plan
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSS	fixed satellite service
FTE	full-time equivalent
FY	fiscal year

## G

GAO	General Accounting Office
GCCS	global command and control system
GEO	geosynchronous earth orbit
GII	global information infrastructure
GIS	geographic information system
GN&C	guidance, navigation, and control
GNP	gross national product
GOTS	government off-the-shelf
GPS	global positioning system
GRI	Gas Research Institute
GSA	General Services Administration
GSO	geostationary earth orbit

**H**

HAZMAT	hazardous materials
HEPA	high-efficiency particulate air (filter)
HEU	highly enriched uranium
HF	high frequency
HHS	Department of Health and Human Services
HQ	headquarters
HSC	Homeland Security Council
HUD	Department of Housing and Urban Development
HVAC	heating, ventilating, and air conditioning

**I**

I3P	Institute for Information Infrastructure Protection
I & C	information and communications
I & W	indications and warnings
IA	information assurance
IAEA	International Atomic Energy Agency
IAP	information assurance program
IAVA	information assurance vulnerability alert
IC	intelligence community
ICC	information coordination center
IDS	intrusion detection system
IEEE	Institute for Electrical and Electronic Engineers
IETS	integrated emergency task force
IITA	Institute for Information Technology Applications
IMPAC	international merchant purchase authorization card
INFOSEC	information security
INMARSAT	International Mobile Satellite Organization
INTERPOL	International Criminal Police Organization
IOC	initial operating capability
IP	internet protocol
IPP	independent power producers
IRIS	integrated risk information system
IRM	information resource management
IRS	Internal Revenue Service
IRT	incident response team
ISAC	information sharing analysis center
ISC	interagency security committee
ISO	independent system operator
ISP	internet service provider
ISR	intelligence, surveillance and reconnaissance
ISSP	information system security program
IT	information technology
ITAA	Information Technology Association of America
ITO	information technology office
IW	information warfare
IWG	interagency working group

**J**

JS	Joint Staff (Department of Defense)
JTTF	Joint Terrorism Task Force

**K**

KAI key asset initiative

**L**

LAN local area network  
 LD 50 lethal dose at which 50 percent of the exposed subjects die  
 LDC local distribution company  
 LEA law enforcement agencies  
 LEC local exchange carrier  
 LEO low earth orbit  
 LEPC local emergency planning committee  
 LFA lead federal agency  
 LNG liquefied natural gas

**M**

MA management agent  
 MEO middle earth orbit  
 MISSI multilevel information system security initiative  
 MIT Massachusetts Institute of Technology  
 MOU memorandum of understanding  
 MPC&A material protection, control, and accounting  
 MSS mobile satellite services/mobile satellite system  
 MST Mountain Standard Time  
 MWS multi-sensor warning systems

**N**

NAREL National Air and Radiation Laboratory  
 NARUC National Association of Regulatory Utility Commissioners  
 NASA National Space Agency  
 NASEO National Association of State Energy Officials  
 NATO North Atlantic Treaty Organization  
 NBC nuclear, biological and chemical  
 NCA National Command Authority  
 NCC National Coordinating Center  
 NCERT National Counter-Terrorism Evidence Response Team  
 NCFL National Computer Forensics Laboratory  
 NCM National Coordinating Measure  
 NCP National Contingency Plan  
 NCS National Communications System  
 NDMS National Disaster Medical System  
 NDPO National Domestic Preparedness Office  
 NEHRP National Earthquake Hazards Reduction Program  
 NEI Nuclear Energy Institute  
 NEIC National Enforcement Investigations Center  
 NEMA National Emergency Management Association  
 NERC North American Electric Reliability Council  
 NETS National Education and Technology Standards  
 NFPA National Fire Protection Association  
 NGI next generation internet  
 NGN next generation network  
 NIAC National Infrastructure Assurance Council  
 NIAID National Institute of Allergy and Infectious Diseases

NIAP	National Information Assurance Partnership
NICT	National Incident Coordination Team
NIETP	National INFOSEC Education and Training Program
NIH	National Institutes of Health
NII	National Information Infrastructure
NIMA	National Imagery Management Agency
NIOSH	National Institute for Occupational Safety and Health
NIPC	National Infrastructure Protection Center
NIPCIP	National Infrastructure Protection and Computer Intrusion Program
NIPRNET	Non-classified Internet Protocol Router Network
NIRT	DoE Nuclear Incident Response Team
NIST	National Institute of Standards and Technology
NIST	National Institute for Standards of Technology
NLETS	National Law Enforcement Telecommunications System
NMCC	National Military Command Center
NMCIAC	New Mexico Critical Infrastructure Assurance Council
NMJIN	National Military Joint Intelligence Command
NNOC	National Network Operations Center
NNSA	National Nuclear Security Administration
NOC	network operation center
NPA	network provider agent
NPC	National Petroleum Council
NPP	nuclear power plant
NRC	National Research Council
NRC	Nuclear Regulatory Commission
NRIC	Network Reliability Interoperability Council
NRO	National Reconnaissance Office
NRT	National Response Team
NS/EP	National Security/Emergency Preparedness
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Directive
NSF	National Science Foundation
NSIE	National Security Information Exchange
NSIRC	National Security Incident Response Center
NSN	National Stock Number
NSSE	National Special Security Event
NSTAC	National Security Telecommunications Advisory Council
NSTAC	National Security Telecommunications Advisory Committee
NTAC	National Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTIA	National Telecommunications and Information Administration
<b>O</b>	
OCA	off-site consequence analysis
OCONUS	Outside Continental United States
ODP	DoJ Office of Domestic Preparedness
OEA	DoE Office of Energy Assurance
OECA	Office of Enforcement and Compliance Assistance
OEI	Office of Environmental Information
OEP	occupant emergency plans

OFX	online financial exchange
OHS	Office of Homeland Security
OIG	Office of the Inspector General
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
OMG	object management group
ONR	Office of Naval Research
OPCON	operational control
OPM	Office of Personnel Management
OSC	on-scene coordinator
OSD	Office of the Secretary of Defense
OSHA	Occupational Safety and Health Administration
OSTP	Office of Science and Technology Policy
OSWER	Office of Solid Waste and Emergency Response

## P

P.L.	Public Law
PAG	protective action guide
PAS	priority access service
PBX	private branch exchange
PC	personal computer
PCA	personal communication agent
PCAST	President's Commission of Advisors on Science and Technology
PCCIP	President's Commission on Critical Infrastructure Protection
PCIPB	President's Critical Infrastructure Protection Board
PCS	personal communications service
PDA	personal digital assistant
PDD	Presidential Decision Directive
PDIT	program development and integration team
PGP	Pretty Good Privacy (popular encryption technology)
PITAC	President's Information Technology Advisory Council
PKI	public key infrastructure
PKI/KMI	public key infrastructure/key management infrastructure
PKIX	public key infrastructure working group
PLMN	public land mobile network
PN	public network
PNNI	private network-to-network interface
POC	point-of-contact
POTUS	President of the United States
PPE	personal protective equipment
PRA	probabilistic risk assessment
PREP	preparedness for emergency response exercise program
PSD	personal security detachment
PST	Pacific Standard Time
PSTN	public switched telecommunications networks
PTS	priority telecommunications system
Pu	plutonium

## Q

Q	queuing
QA	quality analysis
QC	quality control
QoS	quality of service

## R

R&D	research and development
RAL	registered asset list
RAM-D	reliability, availability, maintainability and durability
RDD	radiological dispersal device
RDT&E	research, development, test and evaluation
RECP	regional emergency services communications planner
RERT	radiological emergency response team
RF	radio frequency
RMI	remote method invocation
RMP	risk management plan
RPC	remote procedure call
RRLs	rapid response laboratories
RTO	regional transmission organization

## S

S&T	science and technology
S&IO	security and information operations
S/MIME	secure multipurpose internet mail extensions
S/W	software
SAP	special access program
SBA	Small Business Administration
SCADA	supervisory control and data acquisition
SCIF	sensitive, classified information facility
SDNS	secure domain name service
SEC	Securities and Exchange Commission
SECDEF	Secretary of Defense
SERC	State Emergency Response Commission
SIOC	Strategic Information and Operations Center
SIRT	security incident response team
SMI	security management infrastructure
SMS	short message service
SNM	special nuclear material
SPA	service provider agent
SQL	Structured Query Language
SSA	Social Security Administration
STU	secure telephone unit
STU-III	secure telephone unit-third generation

## T

TACON	tactical command
TCP/IP	transmission control protocol/internet protocol
TDRSS	tracking delay relay satellite system
TDY	temporary duty
TIC	toxic industrial chemical
TMR	tactical mobile robotics
TOA	total obligation authority
TSA	Transportation Security Administration
TSCA	Toxic Substances Control Act
TSP	telecommunications service priority
TSWG	Technical Support Working Group

**U**

UCC	Uniform Commercial Code
UML	Unified Modeling Language
USA DOMS	United States Army Director of Military Support
USACE	United States Army Corps of Engineers
USAMIRIID	United States Army Medical Research Institute for Infectious Diseases
USAO	United States Attorneys' Office
USCG	United States Coast Guard
USCS	United States Customs Service
USDA	United States Department of Agriculture
USG	United States Government
USNCB	United States National Central Bureaus
USNRC	United States Nuclear Regulatory Commission
USPHS	United States Public Health Service
USPS	United States Postal Service
USSPACECOM	United States Space Command
USSS	United States Secret Service
USTRANSCOM	United States Transportation Command

**V**

VA	Veteran's Affairs
VA	Veterans Administration
VAM	Vulnerability Assessment Methodology
VAN	virtual active nodes
VE	virtual environment
VHS	vital human services
VPN	virtual private network

**W**

WAP	wide area protocol
WHO	World Health Organization
WMD	weapons of mass destruction
WPS	wireless priority system

**X**

XML	extensible markup language
-----	----------------------------

**Y**

Y2K	year 2000
-----	-----------



## APPENDIX B

### CRITICAL INFRASTRUCTURE GLOSSARY OF TERMS

The following is a glossary of terms that may be encountered when dealing with critical infrastructure protection issues. While some were used in this publication, several listed here were not but could be encountered in various situations and other publications involving infrastructure protection.

**acceptable risk:** A level of risk that has been determined to be a reasonable level of potential loss or disruption for a specific system.

**access:** The right to enter or use a system and its resources (also given the right to read, write, modify, or delete data) or to use software or network bandwidth.

**access control:** Limiting access to information system resources (processes, programs and other internal systems) to authorized users only.

**advisory:** Assessment of developments or trends regarding threats to a particular system.

**alert:** Notification of an event or combination of events regarding a specific attack directed at a system.

**areas of control:** Protocols designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

**ASIM (automated security incident measurement):** Monitors network traffic and detects unauthorized network activity.

**assessment:** An information acquisition and review process designed to provide input on how to best utilize resources to protect infrastructure systems.

**assurance:** Measure of confidence system can meet its requirements.

**attack:** 1) A discrete malicious action with the intent of inflicting harm/damage upon a system, such as a critical infrastructure, to destroy or incapacitate it.  
2) Intentional attempt to bypass the physical or information security measures and controls protecting an information system

**audit:** Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established security policies and procedures, and/or to recommend necessary changes in controls, policies, or procedures to meet security objectives.

**authenticate:** To establish the validity of a claimed user or object.

**authorization:** Access privileges granted to a user, program, or process.

**automated attack tools:** Software which may be used to attack a remote computer over the Internet.

**backdoor:** A hole in the security of a computer system deliberately left in place by designers or system maintainers, which can be used to circumvent security measures.

**backup:** Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

**bandwidth:** The capacity of a telecommunications link in terms of the amount of data that can be passed through it per second.

**capability:** The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny, or destroy all or part of a critical infrastructure.

**computer network:** A set of connected computers that are able to exchange data.

**confidentiality:** 1) Assurance that information is not disclosed to unauthorized persons, processes, or devices. 2) The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.

**consequence management:** Includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.

**contingency plan:** Plan maintained for emergency response and post-disaster recovery to ensure availability of critical resources and facilitate the continuity of operations in an emergency.

**continuity (of services/operations):** Controls to ensure that, when unexpected events occur, services/operations continue without interruption or are promptly resumed after an event.

**crackers:** Computer experimenters and hobbyists who seek to illegally access secure or unsecured computer networks, hardware, and software for personal or financial gain.

**crisis management:** Includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

**critical asset:** An asset that supports national security, national economic security, and/or crucial public health and safety activities. See also Critical Infrastructure.

**critical infrastructure:** "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." – USA Patriots Act

**cryptography:** The science and technology of keeping information secret from unauthorized parties by use of a mathematical code or cipher.

**cyberspace:** Describes the world of connected computers and the digital environment that resides on it. Also known as the Internet or World Wide Web.

**data integrity:** A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

**denial of service:** 1) A form of attack that reduces the availability of a resource.  
2) Result of any action or series of actions that prevent any part of an information system from providing data or other services to authorized users.

**disaster recovery:** The process of restoring a system to full operation after an interruption in service.

**economic security:** The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens.

**firewall:** A special electronic boundary or access control mechanism (stand-alone computer or software) intended to control access between the Internet and a private computer network.

**hackers:** Computer hobbyists and experimenters who participate in hacking activities.

**hacking:** Exploiting weaknesses in other people's computers to gain unauthorised access to them. (The definition of this term is open to debate. Some people use it mean clever programming with no connotation of breaking security.)

**hardware:** Physical parts of a computer or communications system, as distinct from software.

**incapacitation:** An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact.

**information assurance:** Policy and procedures that protect and defend information and information systems by ensuring their availability, integrity, authentication, and confidentiality. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

**information security:** Actions taken for the purpose of reducing risk to an information system, specifically, reducing the probability that a threat will succeed in exploiting vulnerabilities.

**information sharing and analysis center (ISAC):** Centers designed by the private sector that serve as mechanisms for gathering, analyzing, appropriately sanitizing and disseminating private sector information. These centers could also gather, analyze, and disseminate information from the NIPC for further distribution to the private sector. ISACs also are expected to share important information about vulnerabilities, threats, intrusions, and anomalies, but do not interfere with direct information exchanges between companies and the Government.

**information system:** 1) The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. 2) All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information.

**information technology:** The hardware and software that processes information, regardless of the technology involved, whether computers, telecommunications, or others.

**infrastructure assurance:** Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet expectations despite incurring threat inflicted damage.

**infrastructure protection:** Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures.

**interdependence:** Dependence among elements or sites of different infrastructures, and therefore, effects by one infrastructure upon another.

**internet:** A decentralized, global network of computers (Internet hosts), linked by the use of common communications protocols (Transmission Control Protocol/Internet protocol, or TCP/IP). The Internet allows users worldwide to exchange messages, data, and images. See Cyberspace or World Wide Web.

**internet protocol (IP):** The precise way in which messages are passed through the Internet. All computers connected to the Internet use IP to communicate with each other.

**internet service provider (ISP):** A company that connects businesses and/or individuals to the Internet.

**intranet:** A private network for communications and sharing of information that, like the Internet, is based on TCP/IP but is accessible only to authorized users within an organization.

**intrusion:** Attacks or attempted attacks from outside the security perimeter of an information system.

**mainframe:** A very large computer, used for high-volume high-security applications.

**mitigation:** Pre-planned and coordinated operator reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigatory, and crisis management response; and facilitate reconstitution.

**natural disaster:** A physical capability with the ability to destroy or incapacitate critical infrastructures. Natural disasters differ from threats due to the absence of intent.

**operating system:** A program which control access to a computer and shares its resources among all the other programs it runs. Operating systems are large, complex programs with the potential for many security vulnerabilities. Examples are Microsoft Windows and Unix.

**partnership:** A relationship between two or more entities wherein each accepts responsibility to contribute a specified, but not necessarily equal, level of effort to the achievement of a common goal. For example, the public and private sectors often contribute their relative strengths in a shared effort to protect and assure the continued operation of critical infrastructures.

**patch:** A small change to software already distributed, usually to fix a problem in it.

**physical security:** Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks.

**probe:** Any on-line attempt to gather information about an information system or its users.

**public switched network (PSN):** The term commonly used in the U.S. telecommunications industry and elsewhere for the public telephone system.

**red team:** Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of a system.

**redundancy:** Duplication of system components or personnel intended to increase the reliability of service and/or decrease the risk of loss.

**remote access:** Use of a modem and communications software to connect to a computer network from a distant location via a telephone line or wireless connection.

**response:** Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident.

**risk:** The probability that a particular critical infrastructure's vulnerability will be exploited by a particular threat.

**risk assessment:** A report created to analyze the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities.

**risk management:** Deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level. Characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned value.

**risk-based management:** Risk management that considers unquantifiable, speculative events as well as probabilistic events (taking into account uncertainty as well as risk).

**router:** A piece of hardware that stands at a junction in a computer network and directs messages.

**steganography:** The art and science of communicating in a way that hides the existence of the communication.

**supervisory control and data acquisition (SCADA):** A type of specialised hardware and software used to manage remote parts of power and other networks, particularly water, oil and gas.

**transmission control protocol/internet protocol (TCP/IP):** The basic protocol language underlying the interconnection of computer networks on the internet.

**technology:** 1) Broadly defined, includes processes, systems, models and simulations, hardware, and software. 2) All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.

**threat:** Any circumstance or event with the potential to harm a system through unauthorized access, destruction, and/or denial of service.

**total risk:** The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability).

**trojan horse:** 1) Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

2) A malicious program such as a virus or a worm, hidden in an innocent-looking piece of software, usually for the purpose of unauthorized collection, alteration, or destruction of information.

**virtual private network (VPN):** The use of encryption over a public network to securely link two or more sites.

**virus:** A small, self-replicating, malicious program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed.

**vulnerability:** 1) A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat.  
2) A flaw in security procedures, software, internal system controls, or implementation of an information system that may affect the integrity, confidentiality, accountability, and/or availability of data or services.

**vulnerability assessment:** 1) An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to identify weaknesses that could be exploited or predict the effectiveness of additional security measures in protecting information resources from attack. 2) Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

**vulnerability audit:** The process of identifying and documenting specific vulnerabilities in critical information systems.

**worm:** See virus.





## BACK COVER FLAP

### Quick Facts on U.S. Critical Infrastructure

- Approximately 85% of U.S. infrastructure is privately owned and operated
- 1,912,000+ farms
- 75,000+ state and locally owned dams and reservoirs
- 1,800 federal reservoirs
- 700,000+ miles of drinking water networks
- 170,000+ public drinking water facilities
- 16,000+ publicly owned wastewater treatment facilities
- 5,800+ registered hospitals
- Emergency services/law enforcement organizations in over 87,000 U.S. localities
- 2 billion+ miles of telecommunications cables
- 160,000+ miles of electricity transmission lines
- 2,800+ power plants
- 104 commercial nuclear power plants
- 880,000+ oil wells
- 161 oil refineries
- 220,000+ miles of oil pipeline
- 300,000+ producing natural gas wells
- 1.3+ million miles of natural gas pipelines
- 4,000 offshore platforms
- 600+ natural gas processing plants
- 3.9 million miles of streets, roads and highways
- 100,000+ miles of rail
- Approximately 600,000 bridges
- 361 U.S. ports
- 500 train stations
- 5,000+ public airports
- 66,000+ chemical plants

State Official's Guide to Critical Infrastructure Protection



### Talking Points Card

#### Definition of Critical Infrastructure:

Per the USA Patriot Act, critical infrastructure consists of those “systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.”

#### What do you need to know about Critical Infrastructure?

##### What are the critical infrastructure sectors for states?

- Agriculture/Food
- Water
- Public Health/Emergency Services
- Telecommunications/Information Systems
- Energy
- Transportation
- Banking and Finance
- Chemical Industry

##### Through their continued operation, reliability and resiliency, critical infrastructure ensures the following:

- Production, delivery and distribution of essential goods and services
- Interconnectedness and communications
- Reliability of services
- Public safety and security

##### What problems have states encountered when addressing critical infrastructure protection?

- Infrastructure protection as a new concept
- Information sharing problems
- More focus on response than on protection
- Budget problems

##### What future actions must states take to ensure the protection of critical infrastructure?

- Focus on coordination, communication and information sharing efforts
- Focus on partnerships with other states, the federal government and the private sector
- Conduct protection, readiness and response exercises
- Work on risk assessments and identifying critical assets and vulnerabilities

*Continued on back of card.*



The Council of State Governments